UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

DANIEL GOLDEN and TRACY LOCKE, *Plaintiffs*, v. NEW JERSEY INSTITUTE OF TECHNOLOGY and CLARA WILLIAMS, in her capacity as Custodian of Records for the New Jersey Institute of Technology, *Defendants/Third-Party Plaintiffs/Third-Party Defendants*, v. FEDERAL BUREAU OF INVESTIGATION, *Third-Party Defendant/ Third-Party Plaintiff.*	HON. MADELINE C. ARLEO Civ Action No. 2:15-cv-08559-MCA-LDW

<u>SECOND DECLARATION OF KATIE TOWNSEND IN SUPPORT OF PLAINTIFFS' MOTION FOR ATTORNEYS' FEES</u>

I, Katie Townsend, declare as follows:

1. I am the Litigation Director at the Reporters Committee for Freedom of the Press ("Reporters Committee" or "RCFP"). I have personal knowledge of the matters set forth in this declaration.

2. I am one of the attorneys responsible for representing Plaintiffs Daniel Golden and Tracy Locke (collectively, "Plaintiffs") in the above-captioned case.

3. This second declaration is submitted in support of Plaintiffs' motion for attorneys' fees under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1, *et seq.* ("OPRA" or the "Act").

ADDITIONAL HOURS SPENT BY REPORTERS COMMITTEE ATTORNEYS

4. The attached **Exhibit A** reflects the time spent by Reporters Committee attorneys—specifically by Adam Marshall and myself—reviewing and replying to the opposition filed by defendants/third party plaintiffs/third party defendants New Jersey Institute of Technology and Clara Williams (collectively, "NJIT") to Plaintiffs' motion for attorneys' fees. *See* ECF No. 54.

5. As **Exhibit A** indicates, since Plaintiffs' motion for attorneys' fees was filed on November 30, 2017, Reporters Committee attorneys have spent the following additional number of hours on this matter:

Attorney	**Hours**
Townsend	5.3
Marshall	12.2

6. As **Exhibit A** indicates, these additional hours were spent reviewing and responding to the opposition to Plaintiffs' motion for attorneys' fees that was filed by NJIT on December 21, 2017.

EXHIBITS CITED IN PLAINTIFFS' REPLY BRIEF

7. **Exhibits B through E** hereto are true and correct copies of records that were released to Plaintiffs by NJIT in response to Plaintiffs' OPRA requests that are at issue in this lawsuit. Exhibits B through E are records that were released to Plaintiffs after the filing of the above-captioned lawsuit.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 12th day of January 2018 in Washington, D.C.

Katie Townsend

EXHIBIT A

Date	Matter	Description	User
01/11/2018	Golden v. NJIT	Review revised version of Plaintiffs' reply in support of attorneys' fees motion and make additional changes	Katie Townsend 0.80
01/11/2018	Golden v. NJIT	Drafting/editing Pls' Reply Br ISO attorneys' fees	Adam Marshall 1.10
01/10/2018	Golden v. NJIT	Drafting/editing Pls' Reply ISO Mot. for Attorney's Fees	Adam Marshall 1.70
01/10/2018	Golden v. NJIT	Drafting second Townsend Decl	Adam Marshall 0.60
01/09/2018	Golden v. NJIT	Review/revise draft reply in support of attorneys' fees motion.	Katie Townsend 3.20
01/08/2018	Golden v. NJIT	Review NJIT opposition to attorneys' fees motion and supporting documents (0.8); begin revising draft reply in support of attorneys' fees motion (0.5)	Katie Townsend 1.30
01/05/2018	Golden v. NJIT	Drafting Pls' Reply Br ISO Mot for Attorneys' Fees	Adam Marshall 3.30
01/04/2018	Golden v. NJIT	Drafting Pls' Reply Br ISO Mot for Attorneys' fees	Adam Marshall 4.40
01/03/2018	Golden v. NJIT	Drafting Pls' Reply Br ISO Mot for Attny's fees	Adam Marshall 0.30
01/03/2018	Golden v. NJIT	Legal research re entitlement to attorneys' fees under ORPA	Adam Marshall 0.40
01/03/2018	Golden v. NJIT	Reviewing NJIT's Opp to Pls' Mot for Attorneys' Fees	Adam Marshall 0.50
01/02/2018	Golden v. NJIT	Legal research re third party factual stipulations	Adam Marshall 0.90
			18.50

EXHIBIT B

Subject: RE: SFGate: American Universities Infected by Foreign Spies Detected by FBI
From: [redacted]
Date: 4/10/2012 8:19 AM
To: [redacted]

b6 -1, 2, 3
b7C -1, 2, 3

Dean [redacted]

Thank you for forwarding this article and I am very pleased you enjoyed the symposium. We were hoping to increase everyone's awareness of the issues we face and so far have received positive feedback.

It is a small world and I am glad you had an opportunity to speak with [redacted] [redacted] He is a wonderful agent and person. Please let me know if you need anything.

Take care and thank you again!

Sincerely,
[redacted]
****
Special Agent [redacted]
[redacted]
FBI Newark Division, Trenton RA
[redacted] cell
[redacted]

b6 -1
b7C -1

From: [redacted]
Sent: Monday, April 09, 2012 8:04 AM
To: [redacted]
Subject: FW: SFGate: American Universities Infected by Foreign Spies Detected by FBI

b6 -1, 2, 3
b7C -1, 2, 3

[redacted]

If you have not seen it yet you might be interested in the article below. It might be a good article to put in the packet you give universities.

Your April 3 symposium was excellent. Talk about a small world, [redacted] [redacted] was involved with a company in Biddeford, Maine called Fiber Materials Inc. (FMI) that made nose cones for nuclear weapons by weaving graphite fibers. He mentioned graphite fibers in his talk so I chatted with him later because it so happens I used to work for FMI in the mid-1970s. A few years ago they got caught exporting restricted technology and two folks who I knew quite well were put in jail. One was the guy that hired me.

Best,

[redacted] b6 -2
NJIT b7C -2

This article was sent to you by someone who found it on SFGate.
The original article can be found on SFGate.com here:
http://www.sfgate.com/cgi-bin/article.cgi?file=/g/a/2012/04/08/bloomberg_articlesM1K3W40UQVI901-M24XZ.DTL

Monday, April 9, 2012 (SF Gate)
American Universities Infected by Foreign Spies Detected by FBI
Daniel Golden, ï¿½2012 Bloomberg News

April 9 (Bloomberg) -- Michigan State University President Lou Anna K. Simon contacted the Central Intelligence Agency in late 2009 with an urgent question. The school's campus in Dubai needed a bailout and an unlikely savior had stepped forward: a Dubai-based company that offered to provide money and students. Simon was tempted. She also worried that the company, which had investors from Iran and wanted to recruit students from there, might be a front for the Iranian government, she said. If so, an agreement could violate federal trade sanctions and invite enemy spies. The CIA couldn't confirm that the company wasn't an arm of Iran's government. Simon rejected the offer and shut down undergraduate programs in Dubai, at a loss of $3.7 million. Hearkening back to Cold War anxieties, growing signs of spying on U.S. universities are alarming national security officials. As schools become more global in their locations and student populations, their culture of openness and international collaboration makes them increasingly vulnerable to theft of research conducted for the government and industry. "We have intelligence and cases indicating that U.S. universities are indeed a target of foreign intelligence services," Frank Figliuzzi, Federal Bureau of Investigation assistant director for counterintelligence, said in a February interview in the bureau's Washington headquarters.

'Academic Solicitation'

While overshadowed by espionage against corporations, efforts by foreign countries to penetrate universities have increased in the past five years, Figliuzzi said. The FBI and academia, which have often been at loggerheads, are working together to combat the threat, he said. Attempts by countries in East Asia, including China, to obtain classified or proprietary information by "academic solicitation," such as requests to review academic papers or study with professors, jumped eightfold in 2010 from a year earlier, according to a 2011 U.S. Defense Department report. Such approaches from the Middle East doubled, it said. "Placing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research" in such areas as information systems, lasers, aeronautics and underwater robots, the report said.

World-Class Talent

Welcoming world-class talent to American universities helps the U.S. sustain global supremacy in science and technology, said University of Maryland President Wallace Loh. He chairs the U.S. Department of Homeland Security's academic advisory council, which held its first meeting March 20 and is expected to address such topics as federal tracking of international students. Foreign countries "can never become competitive by stealing," he said. "Once you exhaust that technology, you have to start developing the next generation." Foreigners on temporary visas made up 46 percent of science and engineering graduate students at Georgia Institute of Technology and Michigan State and 41 percent at Massachusetts Institute of Technology in 2009, according to a federal survey. China sent 76,830 graduate students to U.S. universities in 2010-2011, more than any other country and up almost 16 percent from the prior year, according to the Institute of International Education in New York.

Finding Recruits

While most international students, researchers and professors come to the U.S. for legitimate reasons, universities are an "ideal place" for foreign intelligence services "to find recruits, propose and nurture ideas, learn and even steal research data, or place trainees," according to a 2011 FBI report. In one instance described in the report, the hosts of an international conference invited a U.S. researcher to submit a paper. When she gave her talk at the conference, they requested a copy, hooked a thumb drive to her laptop and downloaded every file. In another, an Asian graduate student arranged for researchers back home to visit an American university lab and take unauthorized photos of equipment so they could reconstruct it, the report said. A foreign scientist's military background or purpose isn't always apparent. Accustomed to hosting visiting scholars, Professor Daniel J. Scheeres didn't hesitate to grant a request several years ago by Yu Xiaohong to study with him at the University of Michigan. She expressed a "pretty general interest" in Scheeres's work on topics such as movement of celestial bodies in space, he said in a telephone interview.

Unaware of Credentials

She cited an affiliation with the Chinese Academy of Sciences, a civilian organization, Scheeres said. The Beijing address Yu listed in the Michigan online directory is the same as the Academy of Equipment Command &amp; Technology, where instructors train Chinese military cadets and officers. Scheeres said he wasn't aware of that military connection, nor that Yu co-wrote a 2004 article on improving the precision of anti- satellite weapons. Once Yu arrived, her questions made him uncomfortable, said Scheeres, who now teaches at the University of Colorado. As a result, he stopped accepting visiting scholars from China. "It was pretty clear to me that the stuff she was interested in probably had some military satellite-orbit applications," he said. "Once I saw that, I didn't really tell her anything new, or anything that couldn't be published. I didn't engage that deeply with her."

Wrote About NASA

Yu later wrote a paper on the implications for space warfare of the NASA Deep Impact mission, which sent a spacecraft to collide with a comet. She couldn't be reached for comment. American universities have also trained Chinese researchers who later committed corporate espionage. Hanjuan Jin, a former software engineer at Motorola Inc., was found guilty in February in federal court of stealing the Schaumburg, Illinois-based company's trade secrets and acquitted of charges she did so to benefit China's military. She is scheduled for sentencing in May and has also filed a motion for a new trial. Jin joined the company, now known as Motorola Solutions Inc., after earning a master's degree from the University of Notre Dame in South Bend, Indiana. While at Motorola, she received a second master's, this time in computer science, from the Illinois Institute of Technology in Chicago. IIT's own research wasn't compromised, institute spokesman Evan Venie said in an e-mail. A Notre Dame spokesman declined to comment.

Study Abroad Targets

More Americans are heading overseas for schooling, becoming potential targets for intelligence services, Figliuzzi said. More than 270,000 Americans studied abroad for credit in 2009- 2010, up 4 percent from the year before. President Barack Obama has announced an initiative to send 100,000 American students to China, and China has committed 10,000 scholarships for them. As a junior at Grand Valley State University in Allendale, Michigan, Glenn Duffie Shriver studied at East China Normal University in Shanghai. After graduation, he fell in with Chinese agents, who paid him more than $70,000. At their request, he returned to the U.S. and applied for jobs in the State Department and the CIA. He was sentenced to four years in prison in January 2011 after pleading guilty to conspiring to provide national-defense information to intelligence officers of the People's Republic of China. "Study-abroad programs are an attractive target. Foreign security services find young, bright U.S. kids in science or politics, it's worth winning them over," Figliuzzi said.

Front Companies

Unlike its counterparts in other countries, which rely on their own operatives, China's intelligence service deploys a freelance network including students, researchers and false- front companies, said David Major, president of the Centre for Counterintelligence and Security Studies in Falls Church, Virginia and a former FBI official. China has "lots of students who either are forced to or volunteer to collect information," he said. "I've heard it said, 'If it wanted to steal a beach, Russia would send a forklift. China would send a thousand people who would pick up a grain of sand at a time.'" China also has more than 3,000 front companies in the U.S. "for the sole purpose of acquiring our technology," former CIA officer S. Eugene Poteat, president of the Association of Former Intelligence Officers in McLean, Virginia, wrote in the fall/winter 2006-2007 edition of "Intelligencer: Journal of U.S. Intelligence Studies." U.S. and Canadian universities reaped $2.5 billion in 2011 from licensing technology, up from $222 million in 1991, according to the Association of University Technology Managers in Deerfield, Illinois.

'Opened Some Eyes'

Universities "may not fully grasp exactly who they're spinning off their inventions to," Figliuzzi said. "The company could be a front for a foreign power, and often is. We share specific intelligence with university presidents, and we've opened some eyes." Michigan State's Simon learned to be wary of front companies by serving on the National Security Higher Education Advisory Board, established by the FBI and CIA in 2005. It "makes you more aware that you need to look below the surface of some of these offers," she said. "A short-term solution may turn into an institutional embarrassment." Arizona State University President Michael Crow also sits on the board. "It's all a little perplexing and overwhelming," he said. "We're in the business of trying to recruit more students from China. We're operating at a total openness mode, while we recognize there are people working beyond the rules to acquire information." The Chinese embassy in Washington and the Ministry of Foreign Affairs in Beijing didn't respond to e-mailed questions.

Enabling China

Over the years, American universities have enabled China "to leapfrog into the cutting edge of military capability on the way to superpower status," Richard Fisher, senior fellow on Asian Military Affairs at the International Assessment and Strategy Center in Alexandria, Virginia, said in an e-mail. Chen Dingchang, the head of a Chinese military-sponsored working group on anti-satellite technology, led a delegation in 1998 to the University of Florida to learn about diamond-coating manufacturing, used in missile seekers and other systems, said Mark Stokes, executive director of the Project 2049 Institute in Arlington, Virginia, which studies Chinese aerospace technology. In a 1999 report in a Chinese journal, the authors, including Chen, said the university's cooperation would assist in overcoming a technical bottleneck in China's development of anti-satellite warheads.

'Unlikely to Advertise'

"A university may not know that a visiting engineer could be conducting sponsored research on a military program that could hurt Americans in the event of a conflict," Stokes said. "An engineer supporting a People's Liberation Army program is unlikely to advertise his or her purpose." The University of Florida is "unable to verify" the incident, spokesman Stephen Orlando said. Chen is a technology adviser at China Aerospace Science and Industry Corp., which didn't respond to an interview request. University administrators have traditionally viewed their role as safeguarding academic freedom and making sure that all students, domestic or foreign, are treated the same. "I've been to campuses where deans would say to Chinese students, 'The FBI is coming to talk to you. You have no responsibility to talk to them,'" Major said. "Very hostile environments." Some faculty members remain uneasy about a partnership with federal investigators. "The FBI thrives on a certain degree of paranoia, and it operates in secrecy," said David Gibbs, a history professor at the

University of Arizona. "The secrecy goes against so much of what universities are about, which is openness and transparency."

Stanford University

Stanford University avoids seeking contracts for "export- controlled" research, which only Americans can work on without a license because it has implications for economic or national security. "Stanford does not, nor will it, restrict participation of students on the basis of citizenship," President John Hennessy testified at a January 2010, congressional hearing in Palo Alto, California. More than half of Stanford's doctoral candidates in the physical sciences and engineering come from outside the U.S., he said. Asked by Dana Rohrabacher, a Republican congressman from California, if he had read that Chinese military intelligence uses Chinese students, Hennessy said, "I am aware of that." "Universities need to think that they are patriotic Americans, too," Rohrabacher responded. Hennessy is on sabbatical and unavailable to comment, Lisa Lapin, a Stanford spokeswoman, said in an e-mail.

More Collaboration

After becoming Pennsylvania State University president in 1995, Graham Spanier sought closer collaboration with law enforcement. Reading that a president at another state university expressed shock that a faculty member was under investigation for terrorist ties, he resolved not to be similarly taken aback. He arranged a meeting with representatives of national security agencies including the FBI, CIA, Secret Service and Naval Criminal Investigative Service. "This had never occurred before," Spanier said in a phone interview. "Nobody from higher education had reached out." If they were making inquiries at Penn State, they should let him know, and he would help, Spanier told them. "That began a very fruitful collaboration," he said. Shifting priorities after the Sept. 11, 2001, attacks to terrorism and espionage from organized crime and kidnapping, the FBI expanded the Penn State model into a national board.

Handpicked Board

Spanier approached other university presidents, and 90 percent agreed to serve, he said. Michigan State's Simon took over as chair after Spanier stepped down as Penn State president last November in the wake of a scandal over sex-abuse allegations against a former assistant football coach. Simon and the FBI and CIA have agreed to expand the board and start a subcommittee on cyber-hacking. The FBI handpicks universities for the board, Figliuzzi said. It looks at how much research they conduct, as well as "sensitive cases -- where is there a potential problem? Then we make an invitation." Board members must have security clearances. FBI officials brief them about cases on their campuses, and the presidents in return guide federal investigators through the thickets of higher education.

Problem Solved

When a foreign entity compromised the computer system of a major university, the bureau contacted the school's information- technology administrators, who denied that they had a security breach. The FBI consulted Spanier, who persuaded the university's president to meet with the bureau. "That opened the door to a higher level of cooperation," he said. "The problem was solved." Similarly, the bureau warned Simon that research in behavioral science by a foreign graduate student at Michigan State "might breach the security of corporate America," she said. "We were able to find a way for the student to complete his research and still modify it in a way that took away the national security issues." Beyond resolving such cases, the FBI has also alerted board members to the overall threat, most dramatically through a presentation by a former Russian spy. As a colonel in Russian intelligence and its deputy resident in New York from 1995 to 2000, Sergei Tretyakov set his sights on Columbia University and New York University, according to "Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War" (2008), by Pete Earley.

Mingled With Professors

"We often targeted academics because their job was to share knowledge and information by teaching it to others, and this made them less guarded than, say, UN diplomats," Earley quoted Tretyakov as saying. A typical task was to obtain information about "a study of genetically engineered food being done at New York University." At the board meeting, Tretyakov described to the presidents how Russian spies used to go to campus events and mingle with professors. "It certainly seemed very bold to me that they felt they could interact with faculty and students and attend seminars," Spanier said. "We never really think about that happening on our campuses." In 2009, around the time Tretyakov was briefing the presidents, a Russian spy, Lidiya Guryeva, was pursuing a master's degree in business at Columbia under the name Cynthia Murphy, the 2011 FBI report said. Russian intelligence instructed her to strengthen "ties w. classmates on daily basis incl. professors who can help in job search and who will have (or already have) access to secret info," and to report on their potential "to be recruited by Service." Columbia and NYU declined to comment. Tretyakov died in June 2010. That month, Guryeva was arrested for acting as an agent of a foreign power and deported to Russia.

--With assistance from Natasha Khan in Hong Kong. Editors: Jonathan Kaufman, Lisa Wolfson

To contact the reporter on this story: Dan Golden in Boston at dlgolden@bloomberg.net

To contact the editor responsible for this story: Lisa Wolfson at lwolfson@bloomberg.net

----

EXHIBIT C

Subject: *** POSTPONED *** FBINAA-NJ Chapter 1st Quarter meeting *** POSTPONED ***
From: [redacted]
Date: 1/28/2015 10:03 AM
To: [redacted]

b6 -1
b7C -1

(Note: You are receiving this email due to an interest or pending application for attendance at the FBI National Academy. If you no longer wish to be considered for the National Academy, please advise.)

***** ***** ***** ***** ***** *****

The meeting tonight has been postponed to February 11. Same location and time.

[redacted]
Special Agent
FBI-Newark Field Office
[redacted]
[redacted] *(desk)*
(main)
[redacted]

b6 -1
b7C -1

From: secretary@fbinaanj.org [mailto:secretary@fbinaanj.org]
Sent: Monday, January 26, 2015 4:41 PM
To: Members
Subject: 1st Quarterly Meeting

Dear NJ Chapter Members and invited guests,

Due to the Blizzard that will be impacting the State of New Jersey, it is in our best interest to postpone the First Quarterly Meeting scheduled for Wednesday evening, January 28th.

The re-scheduled date is now February 11th at John Henry's the menu and times remain the same.

I hope all remain safe while we deal with this situation.

Regards,

Michael McCann
2015 President
FBINAA NJ Chapter
Cell [redacted]

b6 -4
b7C -4

EXHIBIT D

Subject: Insider threat materials
From: [redacted]
Date: 6/30/2014 2:21 PM

b6 -1
b7C -1

Good Afternoon,

Please see the attached documents regarding the insider threat.

The attached documents are UNCLASSIFIED. Although UNCLASSIFIED, these reports are not to be released to the media, general public, or posted on any publicly accessible forum, to include the Internet or public websites.

Very respectfully,
[redacted]

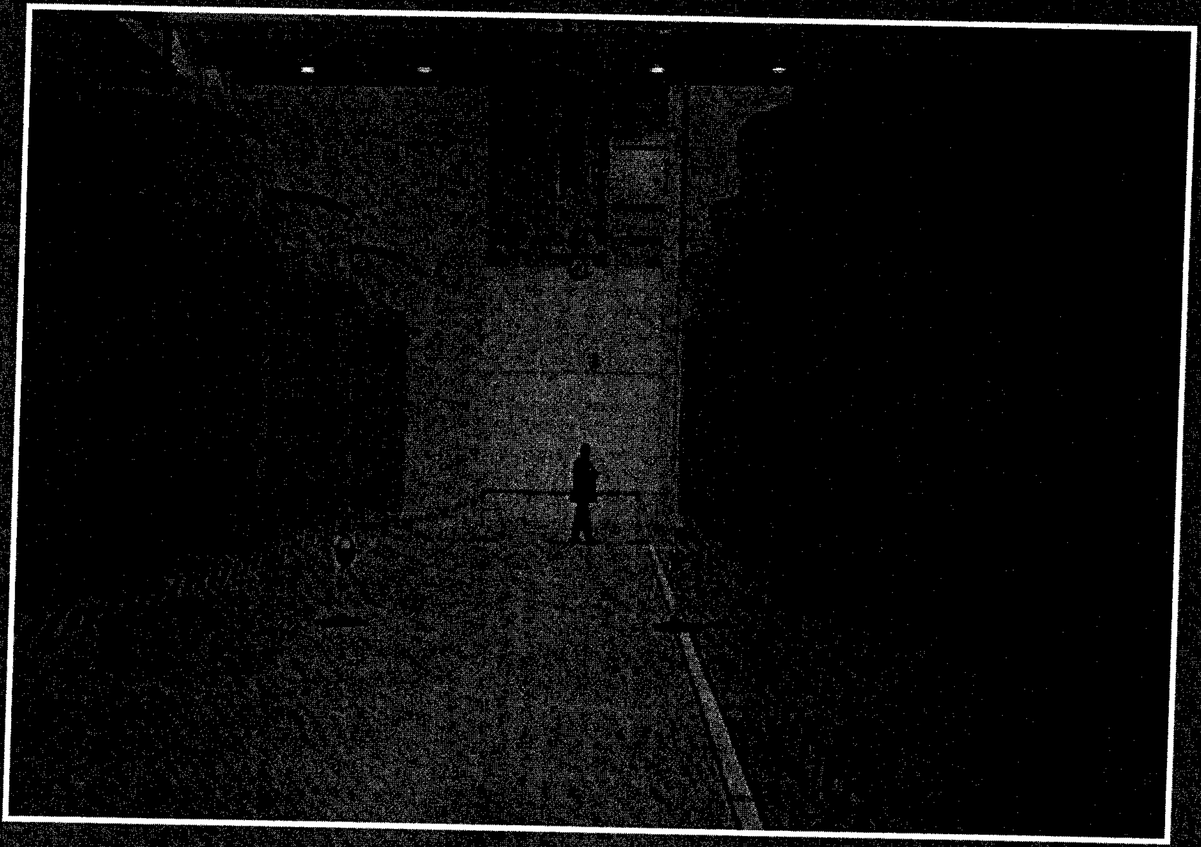
****
Special Agent [redacted]
[redacted]
FBI Newark Division
[redacted] *office*
[redacted]

b6 -1
b7C -1

Attachments:

Worst Practices Guide to Insider Threats - Lessons from Past Mistakes.pdf	203 KB
20140501_Combating the Insider Threat.pdf	1.1 MB

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes



Matthew Bunn and Scott D. Sagan

AMERICAN ACADEMY OF ARTS & SCIENCES

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes

Matthew Bunn and Scott D. Sagan

This publication is available online at http://www.amacad.org/gnf.

Suggested citation: Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014).

Cover image: A man walks inside a newly opened dry spent fuel storage facility.
© Reuters/Stoyan Nenov.

ISBN: 0-87724-097-3

Please direct inquiries to:
American Academy of Arts and Sciences
136 Irving Street
Cambridge, MA 02138-1996
Telephone: 617-576-5000
Fax: 617-576-5050
Email: aaas@amacad.org
Web: www.amacad.org

Contents

Acknowledgments

The authors would like to thank all of the participants in the December 2011 American Academy of Arts and Sciences workshop on Insider Threats held at the Center for International Security and Cooperation (CISAC) at Stanford University. In addition, we thank Roger Howsley, Executive Director of the World Institute of Nuclear Security (WINS), for inviting us to present some of our preliminary findings on this subject at WINS workshops in Vienna, Austria, and in Johannesburg, South Africa. We also express our gratitude to the participants in the CISAC Nuclear Studies Reading Group, sponsored by the John D. and Catherine T. MacArthur Foundation, at which a first draft of this paper was presented, and to the International Atomic Energy Agency for hosting the conference on International Nuclear Security in July 2013, where some of these ideas were also presented.

Matthew Bunn thanks Nickolas Roth and Laura Dismore and Scott Sagan thanks Anna Coll and Reid Pauly for their research assistance related to this paper. Both of us also thank Francesca Giovannini for her superb work as the program officer for the Global Nuclear Future Initiative at the American Academy. Our collaborative work has been made immeasurably better by the dedicated support from and careful research conducted by these talented members of the next generation of international security specialists.

Finally, on behalf of the American Academy of Arts and Sciences, we would like to thank the foundations that have allowed us to work on Insider Threats and on other nuclear related issues throughout the course of the Academy's Global Nuclear Future Initiative. We are deeply grateful to Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, The Alfred P. Sloan Foundation, the Flora Family Foundation, and the Kavli Foundation for their support.

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes

Matthew Bunn and Scott D. Sagan

Insider threats are perhaps the most serious challenges that nuclear security systems face.[1] All of the cases of theft of nuclear materials where the circumstances of the theft are known were perpetrated either by insiders or with the help of insiders; given that the other cases involve bulk material stolen covertly without anyone being aware the material was missing, there is every reason to believe that they were perpetrated by insiders as well. Similarly, disgruntled workers from inside nuclear facilities have perpetrated many of the known incidents of nuclear sabotage. The most recent example of which we are aware is the apparent insider sabotage of a diesel generator at the San Onofre nuclear plant in the United States in 2012; the most spectacular was an incident three decades ago in which an insider placed explosives directly on the steel pressure vessel head of a nuclear reactor and then detonated them.[2] While many such incidents, including the two just mentioned, appear to have been intended to send a message to management, not to spread radioactivity, they highlight the immense dangers that could arise from insiders with more malevolent intent. As

[1] This paper draws on an earlier paper by Scott D. Sagan, "Insider Threats in Comparative Perspective," IAEA-CN-203-156, in *Proceedings of International Nuclear Security: Enhancing Global Efforts*, Vienna, July 1–5, 2013 (Vienna: International Atomic Energy Agency, 2013).

[2] For more on the San Onofre incident, see Jeff Beattie, "Sabotage Eyed in Generator Incident at San Onofre Nuke," *Energy Daily*, December 3, 2012. Engine coolant was found in the oil system of one of the plant's diesel generators—a crucial safety system in the event of loss of off-site power—which would have caused the generator to fail if needed. The plant was shut down at the time. An internal investigation found "evidence of potential tampering as the cause of the abnormal condition," as the company reported to the Nuclear Regulatory Commission (NRC). The explosive attack on the pressure vessel occurred at the Koeberg nuclear power plant in South Africa in 1982, before the plant had begun operating. It was perpetrated by a white South African fencing champion, Rodney Wilkinson, in league with the African National Congress. See, for example, David Beresford, "How We Blew Up Koeberg (. . . and Escaped on a Bicycle)," *Mail & Guardian* (South Africa), December 15, 1995. Beresford has offered a more detailed account, based on interviews with the perpetrator, in *Truth is a Strange Fruit: A Personal Journey Through the Apartheid War* (Auckland Park, South Africa: Jacana Media, 2010), 102–107. We are grateful to Tom Bielefeld for providing this reference. These are but two of a stream of cases that has continued for decades. Three decades ago, an NRC study identified "32 possibly deliberate damaging acts at 24 operating reactors and reactor construction sites" from 1974 to 1980—most of them attributed to insiders. See Matthew Wald, "Nuclear Unit Gets Sabotage Warning," *The New York Times*, June 8, 1983.

it turns out, insiders perpetrate a large fraction of thefts from heavily guarded non-nuclear facilities as well.[3] Yet organizations often find it difficult to understand and protect against insider threats. Why is this the case?

Part of the answer is that there are deep organizational and cognitive biases that lead managers to downplay the threats insiders pose to their nuclear facilities and operations. But another part of the answer is that those managing nuclear security often have limited information about incidents that have happened in other countries or in other industries, and the lessons that might be learned from them.

In the world of nuclear *safety*, sharing of incidents and lessons learned is routine, and there are regularized processes for it, through organizations such as the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO). Nothing comparable exists in nuclear security.[4]

Otto von Bismarck once said that only a fool learns from his mistakes; a wise man learns from the mistakes of others. This paper is intended to help nuclear security operators learn from the mistakes of others in protecting against insider threats, drawing on episodes involving intelligence agencies, the professional military, bodyguards for political leaders, banking and finance, the gambling industry, and pharmaceutical manufacturing. It is based in part on a 2011 workshop hosted by the American Academy of Arts and Sciences at the Center for International Security and Cooperation at Stanford University that brought together experts to compare challenges and best practices regarding insider threats across organizations and industries.

The IAEA and the World Institute for Nuclear Security (WINS) produce "best practices" guides as a way of disseminating ideas and procedures that have been identified as leading to improved security. Both have produced guides on protecting against insider threats.[5] But sometimes mistakes are even more instructive than successes.

Here, we are presenting a kind of "worst practices" guide of serious mistakes made in the past regarding insider threats. While each situation is unique, and serious insider problems are relatively rare, the incidents we describe reflect issues that exist in many contexts and that every nuclear security manager should consider. Common organizational practices—such as prioritizing production over security, failure to share information across subunits, inadequate rules or inappropriate waiving of rules, exaggerated faith in group loyalty, and excessive

[3] Bruce Hoffman, Christina Meyer, Benjamin Schwarz, and Jennifer Duncan, *Insider Crime: The Threat to Nuclear Facilities and Programs* (Santa Monica, Calif.: RAND, 1990).

[4] Matthew Bunn, "Strengthening Global Approaches to Nuclear Security," IAEA-CN-203-298, in *Proceedings of International Nuclear Security: Enhancing Global Efforts*, Vienna, July 1–5, 2013 (Vienna: International Atomic Energy Agency, 2013).

[5] International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, Security Series No. 8 (Vienna: IAEA, 2008); and World Institute for Nuclear Security, *Managing Internal Threats: A WINS International Best Practice Guide for Your Organization* (Vienna: WINS, 2010).

focus on external threats—can be seen in many past failures to protect against insider threats.

LESSONS

Lesson #1: Don't Assume that Serious Insider Problems are NIMO (Not In My Organization)

Some organizations, like companies in the diamond-mining industry or the gambling industry, assume that their employees may be thieves. They accept that relatively low-consequence insider theft happens all the time, despite employee screening and inspections designed to prevent it.

By contrast, organizations that consider their staff to be part of a carefully screened elite—including intelligence agencies and many nuclear organizations, among others—often have strong internal reasons to stress and reinforce the loyalty and morale of their employees in order to encourage more effective operations. They also sometimes have incentives to encourage perceptions that competitors do not have the same levels of loyalty. The repeated stress on the high loyalty of one's organization when compared to others can lead management to falsely assume that insider threats may exist in other institutions, but not in their organization.

A dramatic case in point was the failure to remove Sikh bodyguards from Indian Prime Minister Indira Gandhi's personal security unit after she had instigated a violent political crackdown on Sikh separatists in 1984. In June 1984, Operation Blue Star targeted Sikh separatists who had taken over the Golden Temple in Amritsar.[6] Extra security personnel were deployed at the prime minister's residence after a series of death threats were made against the prime minister and her family. According to H. D. Pillai, the officer in charge of Gandhi's personal security, "[T]he thrust of the reorganized security . . . was to prevent an attack from the outside. . . . What we did not perceive was that an attempt would be made inside the Prime Minister's house."[7] When it was suggested by other officials that Sikh bodyguards should be placed only on the outside perimeter of the prime minister's compound, Mrs. Gandhi insisted that this could not be done without damaging her political reputation: "How can I claim to be secular if people from one community have been removed from within my own house?"[8] On October 31, 1984, two Sikh guards—one a long-standing bodyguard (Beant Singh, the personal favorite of Mrs. Gandhi) and the other a newly added guard (Satwant Singh)—conspired and assassinated Mrs. Gandhi.

[6] For more detail, see Scott D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Security," *Risk Analysis* 24 (4) (2004): 935–946.

[7] Ritu Sarin, *The Assassination of Indira Gandhi* (New Delhi: Penguin, 1990), 19.

[8] Ibid.

The Gandhi case, unfortunately, was not unique. While Pervez Musharraf was president of Pakistan, he survived at least two near-miss assassination attempts, both of which were perpetrated by active Pakistani military personnel in league with al-Qaeda.[9] Similarly, Ahmed Wali Karzai, a powerful Afghan regional official and the brother of the Afghan president, was assassinated in 2011 by his principal security guard, a trusted confidant who had worked with the family for seven years.[10]

These cases offer several key lessons. First, and most fundamentally, organizational leaders should never assume that their personnel are so loyal that they will never be subject to ideologies, shifting allegiances, or personal incentives that could lead them to become insider threats. Managers should beware of the "halo effect," in which well-liked employees are assumed to be trustworthy (a special case of *affect bias*, the tendency we all have to assume that something we like for a particular reason has other positive qualities as well).[11]

Second, managers should understand that guards themselves can be part of the insider threat—"the most dangerous internal adversaries," in the words of a senior Russian nuclear security manager.[12] Indeed, according to one database, guards were responsible for 41 percent of insider thefts at non-nuclear guarded facilities.[13] Hence, managers should not assume that adding more guards automatically leads to increased security.[14] Finally, individual leaders or facility managers should not countermand security professionals' judgments solely for personal or political reasons.

Lesson #2: Don't Assume that Background Checks will Solve the Insider Problem

The belief that personnel who have been through a background check will not pose an insider problem is remarkably widespread—a special case of the "not in my organization" fallacy. There are two reasons why this belief is mistaken. First, background checks are often not very effective. Second, even completely trustworthy employees may become insiders, especially if they are coerced.

[9] See, for example, "Escaped Musharraf Plotter Was Pakistan Air Force Man," *Agence France Presse*, January 12, 2005; and "Musharraf Al-Qaeda Revelation Underlines Vulnerability: Analysts," *Agence France Presse*, May 31, 2004.

[10] Bashir Ahmad Naadem, "Suspects Arrested in Wali Assassination," *Pajhwok Afghan News*, July 12, 2011.

[11] For the halo effect, see Richard E. Nisbett and Timothy D. Wilson, "The Halo Effect: Evidence for Unconscious Alteration of Judgments," *Journal of Personality and Social Psychology* 35 (4) (April 1977): 250–256. For a discussion of affect bias (and other biases likely to be important to nuclear security managers), see Daniel Kahneman, Paul Slovic, and Amos Tversky, eds., *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982).

[12] Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii [Reforming MVD Troops to Guard Russian Nuclear Facilities]," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9 (4) (Winter 2003).

[13] Hoffman et al., *Insider Crime.*

[14] Sagan, "The Problem of Redundancy Problem."

Background checks as they are conducted today often fail to catch indicators of potential problems. Even in-depth, ongoing monitoring can miss key insider issues: after all, Aldrich Ames famously passed lie detector tests. Moreover, in many cases at non-nuclear facilities, there was no indication that employees were not trustworthy until long after they were hired: they became criminals only once on the job. This was the case with the trusted guards discussed in the previous section; and Leonid Smirnov, who perpetrated one of the first well-documented thefts of weapons-usable nuclear material (1.5 kilograms of 90 percent enriched HEU from the Luch Production Association in Podolsk in 1992), was a trusted employee who had worked at the facility for many years.[15]

Even if all the insiders at a facility are highly reliable, coercion remains a danger. In a case in Northern Ireland in 2004, for example, thieves allegedly linked to the Provisional Irish Republican Army made off with £26 million from the Northern Bank. The bank's security system was designed so that the vault could be opened only if two managers worked together, but the thieves kidnapped the families of two bank managers and blackmailed them into helping the thieves carry out the crime.[16] (The thieves also used deception in this case, appearing at the managers' homes dressed as policemen.) No background check or ongoing employee monitoring system can prevent insiders from acting to protect their families. Terrorists (as the Northern Bank thieves may have been) also make use of such coercion tactics, and might do so to enlist help in a theft of nuclear material, rather than money. For example, kidnapping in order to blackmail family members into carrying out certain actions has been a common Chechen terrorist tactic.[17] An examination of a range of major crimes concluded that such coercion tactics are frequently successful.[18]

The lesson here is clear: while it is important to have programs that screen employees for trustworthiness and monitor their behavior once employed, no one should ever assume that these programs will be 100 percent effective. Measures to prevent insider theft are needed even when a manager believes all of his employees are likely to be completely trustworthy.

[15] For interviews with Smirnov, see *Frontline*, "Loose Nukes: Interviews" (Public Broadcasting System, original air date November 19, 1996), http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/; and Ginny Durrin and Rick King, *Avoiding Armageddon*, episode 2, "Nuclear Nightmares: Losing Control" (Ted Turner Documentaries, 2003), http://www.pbs.org/avoidingarmageddon.

[16] For a good introduction to the Northern Bank case, see Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life*, May 21, 2006. One of the managers, Chris Ward, was subsequently charged with being a willing participant in the crime, and the kidnapping of his family a sham. Ward denied the charges and was subsequently acquitted. See Henry McDonald, "Employee Cleared of £26.5 Million Northern Bank Robbery," *Guardian*, October 9, 2008.

[17] Robyn Dixon, "Chechnya's Grimmest Industry: Thousands of People Have Been Abducted by the War-Torn Republic's Kidnapping Machine," *Los Angeles Times*, September 18, 2000.

[18] Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-1498-SL (Santa Monica, Calif.: RAND, 1980).

Lesson #3: Don't Assume that Red Flags will be Read Properly

High-security facilities typically have programs to monitor the behavior of employees for changes that might suggest a security issue, and to encourage other employees to report such changes. Effective personnel screening, training, and monitoring systems are designed to pick up subtle signs that personnel reliability has been or is about to be compromised by disgruntlement, mental health problems, drug abuse, or personal life difficulties, or that security reliability has been or is about to be compromised by shifting political allegiances, corruption, recruitment, or self-radicalization. While picking up subtle signs of danger is difficult, security managers often assume that severe red flags warning of problems will not go unnoticed. But if individual incentive systems and information-sharing procedures encourage people not to report, even the reddest of red flags can be ignored.

The shooting incident at Fort Hood, Texas, is an extreme version of this problem. On November 5, 2009, U.S. Army Major Nidal Hasan opened fire on a group of soldiers preparing to deploy to Afghanistan, killing thirteen and wounding twenty-nine.[19] Major Hasan had made no secret of his radicalized, violent beliefs, voicing his justification of suicide bombers, defense of Osama bin Laden, and devotion to Sharia law over the U.S. Constitution to peers and supervisors over a period of *years* before the attack. The San Diego Joint Terrorism Task Force (JTTF), an interagency group managed by the FBI, had also obtained multiple email communications between Hasan and a "foreign terrorist" reported in the press to be Anwar al-Awlaki.[20] As Amy Zegart has argued, stopping "a radicalized American Army officer who was publicly espousing his beliefs and was known to be communicating with one of the world's most dangerous and inspirational terrorists in the post-9/11 era was not asking the impossible."[21]

Why did multiple U.S. government processes fail to act on the obvious red flags raised by Hasan? There were several reasons. First, the process for review and removal of an officer on security reliability grounds was time-consuming and cumbersome, posing an immense set of headaches to anyone who tried to act. Combined with the incentive to keep someone with Hasan's psychiatry specialty in the service, no officer at Walter Reed decided to start proceedings against Hasan. Second, the Army's system for reviewing officers' performance

[19] This case study is based on Amy Zegart, "The Fort Hood Terrorist Attack: An Organizational Postmortem on DOD and FBI Deficiencies," working paper, March 20, 2013.

[20] U.S. Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, Special Committee Report [hereafter Senate Report], 112th Cong., 1st sess., February 3, 2011, pp. 28–31; Sebastian Rotella and Josh Meyer, "Fort Hood's Suspect Contact with Cleric Spelled Trouble, Experts Say," *Los Angeles Times*, November 12, 2009; Carrie Johnson, "FBI to Probe Panels that Reviewed Emails from Alleged Fort Hood Gunman," *The Washington Post*, December 9, 2009; and Carrie Johnson, Spencer S. Hsu, and Ellen Nakashima, "Hasan had Intensified Contact with Cleric," *The Washington Post*, November 21, 2009.

[21] Zegart, "The Fort Hood Terrorist Attack."

failed to compile the relevant information in a usable way. There were two sets of files for each officer. Personal files were quite detailed, but kept only at the local level and destroyed when a service member moved on, making it impossible to track behavior from one assignment to the next. Officer Evaluation Reports (OERs) had only yes/no judgments on standardized questions, combined with an overall rating of an officer's suitability for promotion; given the shortage of middle-grade officers in the post–Cold War military, there were substantial pressures not to make trouble by giving poor ratings, and every OER that Hasan received was positive, despite his alarming statements and abysmally poor performance in his job. As a Senate investigation found, Hasan's reviews "flatly misstated" his actual performance and made no mention of the red flags he was repeatedly raising.[22] Third, as often happens in organizational settings, significant social shirking occurred, as there was ample opportunity to pass difficult responsibilities on to someone else. Hasan was moving soon from Walter Reed to Fort Hood, and officers at the former base knew that as long as they did nothing to raise any issues about his transfer, they would not have to deal with him anymore. (The wonderful phrase used to describe the practice of writing positive reviews of poor-performing service members so that they can be shipped to another command is "packaged for export.") Fourth, at least some officers feared that actions taken to discipline a Muslim officer for his political statements would have been perceived as discriminatory.

Fifth, there was a severe lack of information sharing between Army security specialists and the JTTF, which had responsibility for evaluating the intercepted email messages between Hasan and al-Awlaki, and between different JTTF offices. The San Diego JTTF wanted an investigation of the email communication that it had found, but the Washington office had jurisdiction and did not give Hasan as high a priority as the San Diego office thought justified. Due to problems with their information systems and misunderstandings between them, both the San Diego JTTF and the Washington JTTF thought the other was monitoring Hasan's continued communications, when in fact neither was. In the end, the only investigation that the Washington JTTF performed was a review of Hasan's OERs, which found only positive reports—and "some even sanitized his obsession with Islamic extremism as praiseworthy research."[23] No one looked at Hasan's local records, interviewed him, or spoke to any of his colleagues or superiors. Hence, a junior Department of Defense official in the Washington JTTF, after reviewing the positive OERs, made the tragic and controversial decision that Hasan's email conversations with al-Awlaki were just part of a research project; he therefore did not feel the need to pass on the intelligence reports to Hasan's superior officers.

The lessons here are disturbing. When individual and group incentives push against objective analysis of warning signals, and when, as often happens

[22] Discussed in ibid.

[23] Ibid.

in compartmentalized security organizations, information sharing is restricted, even the reddest of red flags can be ignored.

Nuclear managers may assume that their systems for detecting red flags are much better—that they would surely catch someone like Hasan. But the case of Sharif Mobley suggests that this may not always be the case. In March 2010, Mobley was arrested in Yemen for alleged involvement in al-Qaeda and for shooting a guard in an attempt to escape. Yet between 2002 and 2008, prior to traveling to Yemen, Mobley worked at five U.S. nuclear power plants (Salem-Hope Creek, Peach Bottom, Limerick, Calvert Cliffs, and Three Mile Island), where he was given unescorted access inside the plant (though not in the vital areas) to perform maintenance and carry supplies. According to a Nuclear Regulatory Commission (NRC) report, Mobley voiced his militant views during his work, referring to non-Muslim coworkers as "infidels" and remarking to some in his labor union: "We are brothers in the union, but if a holy war comes, look out."[24] Though the rules in place at the time required individual workers to report any suspicious behavior on the part of coworkers, none of Mobley's fellow union members apparently reported these statements. The red flags were again invisible.

Cases of ignoring red flags as extreme as Hasan's, or even Mobley's, do not happen often. But the issues raised—failing to report problems because of the headaches involved, passing troublesome employees off to someone else—arise in smaller ways in almost every organization. Indeed, research suggests that indicators of insider security problems are systematically underreported.[25] One study of several cases of insider information-technology sabotage in critical infrastructure found that 97 percent of the insiders involved in the cases "came to the attention of supervisors or coworkers for concerning behavior prior to the attack," but the observed behavioral precursors were "ignored by the organization."[26]

All managers of nuclear organizations should be asking themselves: how are the incentives for reporting such issues *really* aligned in my organization? How could I test how well such issues are reported? How could I improve my organization's ability to detect and act on a potential problem before it occurs?

[24] Scott Shane, "Worker Spoke of Jihad, Agency Says," *The New York Times*, October 4, 2010, http://www.nytimes.com/2010/10/05/us/05mobley.html?_r=0 (accessed May 19, 2013); and Peter Finn, "The Post-9/11 Life of an American Charged with Murder," *The Washington Post*, September 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/04/AR2010090403334.html (accessed May 19, 2013).

[25] Suzanne Wood and Joanne C. Marshall-Mies, *Improving Supervisor and Co-Worker Reporting of Information of Security Concern* (Monterey, Calif.: Defense Personnel Security Research Center, January 2003). Subsequently, researchers from the same center developed an improved reporting system now used in the Department of Defense, and the reporting system may be of interest to nuclear security managers. See Suzanne Wood, Kent S. Crawford, and Eric L. Lang, *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers* (Monterey, Calif.: Defense Personnel Security Research Center, May 2005).

[26] Andrew P. Moore, Dawn M. Capelli, and Randall F. Trzeciak, *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*, CMU/SEI-2008-TR-2009 (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, May 2008).

Lesson #4: Don't Assume that Insider Conspiracies are Impossible

Conspiracies of multiple insiders, familiar with the weaknesses of the security system (and in some cases including guards or managers), are among the most difficult threats for security systems to defeat. Many nuclear security systems include only a single insider in the threats they are designed to protect against. And many nuclear security experts do not see groups of insiders as a credible threat: in a recent survey of nuclear security experts from most of the countries where HEU and separated plutonium exist, most agreed that a single insider was a highly credible threat; but no one rated multiple insiders as highly credible, and only a few rated insider conspiracies as "somewhat credible."[27]

Yet insider conspiracies routinely occur. In one database, they constituted approximately 10 percent of the crimes examined.[28] In 1998, for example, an insider conspiracy at one of Russia's largest nuclear weapons facilities attempted to steal 18.5 kilograms of HEU—potentially enough for a bomb.[29] The Northern Bank case described above is another example, involving two trusted, senior insiders working together—both under coercion from threats to their families. The Gandhi case is yet another example—again involving two insiders working together, both trusted enough to be personal guards to the prime minister. The fact that two of the major cases selected above to illustrate other points also involved insider conspiracies is a telling indicator of how important such conspiracies are.

The lesson here is clear: wherever possible, nuclear security systems should be designed to offer substantial protection against even a small group of insiders working together. Nuclear security managers should set up "red team" processes for identifying approaches that groups of insiders might use to steal material and for finding cost-effective approaches to stop them.

Lesson #5: Don't Rely on Single Protection Measures

Many managers have high confidence in particular elements of their security system, from a particularly well-trained guard force to portal monitors at every exit. Many such systems, however, are much more vulnerable to being defeated

[27] Matthew Bunn and Eben Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (Cambridge, Mass.: Project on Managing the Atom, Harvard Kennedy School, March 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.

[28] Hoffman et al., *Insider Crime*.

[29] This attempt was first revealed by the Russian Federal Security Service (FSB), which claimed credit for foiling it. See Yevgeniy Tkachenko, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, December 18, 1998. The attempt was discussed in somewhat more detail by Victor Erastov, chief of material accounting for what was then Russia's Ministry of Atomic Energy; see "Interview: Victor Yerastov: MINATOM Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest* 5 (1) (Winter 2000). Neither of those accounts identified the type of material; that is from a 2000 interview by Matthew Bunn with a Ministry of Atomic Energy official.

than they first appear—especially to insiders, who may be among the staff who know how they work.

Portal monitors are one example; they are essential but imperfect. In discussion with Matthew Bunn, a Livermore security expert described a meeting with representatives of a portal-monitor production firm who had very high confidence in their product's ability to detect nuclear material. The company gave the security expert a radioactive test sample that they were confident their system could detect, and in three times out of five, he was able to carry it through the monitor without detection.

Or consider the case of tamper-indicating devices (TIDs), also known as seals, widely used to indicate whether any material has been removed or tampered with. Many people believe that an unbroken seal shows with high confidence that the sealed item has not been disturbed. Yet a study of 120 types of seals in common commercial and government use found that all 120 could be defeated in ways that would not be detected by the seal inspection protocols in use. Tampering was possible with materials available from any hardware store, and with defeat times averaging about five minutes.[30] The TIDs included sophisticated fiber-optic seals, among others; some of these high-tech options did not perform as well, when used as people in the field actually use them, as lower-tech methods.

In short, security managers should never have too much faith in any one element of their security system. Seals can be defeated, portal monitors can be defeated or gone around, guards can fail to search employees, employee reporting systems can fail to detect suspicious behavior. But with a system that genuinely offers defense in depth, it can be made very difficult for an insider adversary to overcome all the layers in the system.

Lesson #6: Don't Assume that Organizational Culture and Employee Disgruntlement Don't Matter

Nuclear organizations often have an engineering culture, focused more on the technology than on the people using it. Managers sometimes assume that as long as the right systems and procedures are in place, employees will follow the procedures and everything will be fine. In most countries, including the United States, regulators do not require operators to take any steps to ensure a strong security culture, or even to have a program to assess and improve security culture that regulators can review.

But the reality is that the culture of an organization and the attitudes of the employees have a major impact on security. As General Eugene Habiger, former Department of Energy "security czar" and former commander of U.S. strategic forces, put it, "Good security is 20 percent equipment and 80 percent culture."[31]

[30] Roger G. Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," *Science & Global Security* 9 (2001): 93–112.

[31] From an April 2003 interview by Matthew Bunn.

A visit by Matthew Bunn to a Russian nuclear institute in the mid-2000s provides an example of the impact of security culture on insider protection. In the hallway leading to the vault where a substantial amount of weapons-grade nuclear material was stored, there were two portal monitors that personnel had to pass through, one after the other, an American machine and a Russian machine. When asked why, the site official conducting the tour said that the building next door made medical isotopes, and on Thursdays, when the chemical separations were done to get the desired isotopes from the remainder, so much radiation went up the stack that it set off the American-made portal monitor. So on Thursdays, they turned off the American-made monitor and relied on the less sensitive Russian one. Of course, every insider was aware of this practice, and would know to plan an attempted theft for a Thursday, making the existence of the American portal monitor largely pointless.

A photograph from a 2001 U.S. General Accounting Office report provides a similar example: it shows a wide-open security door at a Russian facility. What is remarkable is that the door was propped open on the very day the American auditors were there to photograph it being propped open, suggesting that the staff did not see this as a problem.[32]

Perhaps the most spectacular recent incident caused by a breakdown of security culture was the intrusion by an 82-year-old nun and two other protesters at the Y-12 facility in Tennessee in 2012. The protesters went through four layers of fences, setting off multiple intrusion detectors, but no one bothered to check the alarms until the protesters had spent some time hammering and pouring blood directly on the wall of a building where enough weapons-grade HEU metal for thousands of nuclear weapons is stored. As it turns out, a new intrusion detection system had been setting off ten times as many false alarms as the previous system had, yet this was tolerated; cameras to allow guards to assess the cause of the alarms had been broken for months, and this was also tolerated. The guards apparently had gotten sick of checking out all the alarms, and even the heavily armed guards inside the building did not bother to check when they heard the hammering, assuming that it must have been construction work they had not been told about (even though this all took place before dawn).[33]

To avoid such problems, nuclear managers should seek to build a culture in which all employees take security seriously and count it as an important part of their mission—all day, every day. They must also foster employees' understanding that security is everyone's responsibility, not something only the security

[32] U.S. Congress, General Accounting Office, *Security of Russia's Nuclear Material Improving, More Enhancements Needed*, GAO-01-312 (Washington, D.C.: GAO, February 2001).

[33] See, for example, C. Donald Alston, Letter to Secretary of Energy Steven Chu, December 10, 2012, http://pogoarchives.org/m/nss/20121210-alston-ltr.pdf; Norman Augustine, Letter to Secretary of Energy Steven Chu, December 6, 2012, http://pogoarchives.org/m/nss/20121210-augustine-ltr.pdf; Richard Meserve, Letter to Secretary of Energy Steven Chu, December 6, 2012, http://pogoarchives.org/m/nss/20121206-meserve-ltr.pdf; and Office of the Inspector General, U.S. Department of Energy, *Inquiry Into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, DOE/IG-0868 (Washington, D.C.: DOE, August 2012), http://energy.gov/sites/prod/files/IG-0868_0.pdf.

team has to worry about.[34] Establishing clear incentives that make employees understand that they will be rewarded for good security performance is one key element of building such a culture, and of making clear the priority that management places on security.[35]

Employee satisfaction is another critical aspect of organizational culture. Disgruntled employees are much more likely to become insiders—and much less likely to proactively help to improve security by reporting odd or suspicious behavior or by creatively looking for security vulnerabilities and ways to fix them. In situations ranging from retail theft to IT sabotage, disgruntlement has been found to be a key driver of insider threats.

In the study of IT sabotage cases mentioned above, the authors found that 92 percent of the cases examined occurred "following a negative work-related event such as termination, dispute with a current or former employer, demotion, or transfer." Well over half of the insiders in these cases were already perceived in the organization to be disgruntled.[36]

Fortunately, organizations have found that it is not very difficult or expensive to combat employee disgruntlement. Providing complaint and ombudsman processes that are perceived to result in actions to address the issues; complimenting and rewarding employees for good work; addressing the problem of bullying bosses: these and other steps can go a long way toward reducing disgruntlement and its contribution to the insider threat.[37]

It is not known how much of a contribution disgruntlement makes to the probability of an insider taking more serious actions, such as stealing nuclear material or sabotaging a nuclear facility. Nevertheless, for both safety and security reasons, nuclear managers should strive to build a strong, performance-oriented culture in which employees believe that they are respected and treated well, and in which they have avenues for their complaints and ideas to be heard.

Lesson #7: Don't Forget that Insiders May Know about Security Measures and How to Work Around Them

Many individuals involved in the nuclear security field have backgrounds in engineering and nuclear safety, where the goal is to protect against natural disasters and accidents, not against reactive adversaries. This can produce a compliance-oriented approach to security: a belief that once systems are in place

[34] On the importance of this point, see World Institute for Nuclear Security, *Nuclear Security Culture: A WINS Best Practice Guide for Your Organization*, revision 1.4 (Vienna: WINS, September 2009).

[35] Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management*, Phoenix, Ariz., July 10–14, 2005 (Northbrook, Ill.: INMM, 2005); available at http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf.

[36] Moore, Capelli, and Trzeciak, *The "Big Picture" of Insider IT Sabotage.*

[37] See Roger G. Johnston, "Mitigating the Insider Threat (and Other Security Issues)," http://www.ne.anl.gov/capabilities/vat/pdfs/Insider%20Threat%20and%20Other%20Security%20Issues.pdf.

that are assessed to be capable of beating the adversaries included in the design basis threat (DBT) on the pathways designers identified, the security system will be effective. But reactive adversaries will observe the security systems and the pathways they protect against, and they will think of other pathways. Insider threats are a particularly dangerous form of reactive adversary because insiders are well placed to understand the organization's security procedures and their weaknesses.

The best case to illustrate this point is that of Robert Hanssen, the senior FBI analyst convicted in 2001 on fifteen counts of espionage, in what the FBI has called "possibly the worst intelligence disaster in U.S. history."[38] According to the 2003 Department of Justice report on the case, Hanssen's initial decision to engage in espionage "arose from a complex blend of factors, including low self-esteem and a desire to demonstrate intellectual superiority, a lack of conventional moral restraints, a feeling that he was above the law, a lifelong fascination with espionage and its trappings and a desire to become a 'player' in that world, the financial rewards he would receive, and the lack of deterrence—a conviction that he could 'get away with it.'"[39] His espionage activities often raised alarm bells, but his insider advantage let him avoid detection in three key ways. First, Hanssen was capable of being uniquely reactive to counterintelligence investigations because of his placement within the FBI counterintelligence bureaucracy. Second, Hanssen was able to alter his contact procedures with his Russian associates whenever he felt that he was close to being caught; he was even able to search for his own name within the FBI internal database to monitor whether he was the subject of any investigation.[40] Third, Hanssen knew how to avoid movement within the FBI bureaucracy that would have subjected him to polygraph examinations.[41]

In other contexts, this problem—that insiders can observe and work around security measures—comes up again and again. In a study of insider crimes that might be analogous to insider thefts or attacks at nuclear facilities, the authors repeatedly found that the success of insider crimes depended on the perpetrators' observation of security vulnerabilities.[42] The study of insider IT sabotage mentioned earlier noted that the insiders overwhelmingly took advantage of their knowledge of the IT security systems, creating access pathways for them-

[38] U.S. Department of Justice, Commission for Review of FBI Security Programs, "A Review of FBI Security Programs," March 2002, http://www.fas.org/irp/agency/doj/fbi/websterreport.html (accessed May 17, 2013).

[39] U.S. Department of Justice, "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen," August 2003, http://www.justice.gov/oig/special/0308/final.pdf (accessed May 17, 2013).

[40] Ibid.

[41] David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House, 2002), 177.

[42] Hoffman et al., *Insider Crime.*

selves completely unknown to the organization—in other words, they invented ways to attack that the security planners had not known were possible.[43]

There are several lessons here. First, security managers need to find creative people with a hacker's mindset to come up with a wide range of ways that insiders might try to beat the security system—and then develop security measures that will be effective against a broad range of possibilities. A security system adequate to defend against the first few pathways thought of by an unimaginative committee is not likely to be good enough against the real threat. Such uncreative vulnerability assessments were the target for Roger Johnston and his colleagues in the Vulnerability Assessment Team at Argonne National Laboratory; in their instructive and amusing set of "Security Maxims," they offer the "Thanks for Nothin'" maxim: "Any vulnerability assessment which finds no vulnerabilities or only a few is worthless and wrong."[44] Second, those with the most detailed information about how the organization protects itself against insider threats should be subject to especially strong reviews and monitoring to ensure that the organization is appropriately "guarding the guardians."

Lesson #8: Don't Assume that Security Rules are Followed

Security-conscious organizations create rules and procedures to protect valuable assets. But such organizations also have other, often competing, goals: managers are often tempted to instruct employees to bend the security rules to increase productivity, meet a deadline, or avoid inconvenience. And every hour an employee spends following the letter of security procedures is an hour not spent on activities more likely to result in a promotion or a raise.[45] Other motivations—friendships, union solidarity, and familial ties—can also affect adherence to strict security rules.

The cases here are legion; indeed, any reader who has worked for a large organization with security rules probably has direct experience of some of those rules being violated. In many cases, the security rules are sufficiently complex and hard to understand that employees violate them inadvertently. In some cases, the deviations from the rules are more substantial. In both the United States and Russia, for example, there have been cases of nuclear security guards sleeping on the job; patrolling without any ammunition in their guns (apparently because shift managers wanted to ensure that there would be no accidental firing incidents on their watch); and turning off intrusion detection systems when they got tired of checking out false alarms (arguably even worse than simply ignoring those alarms, as appears to have occurred in the Y-12 case). In one U.S. case prior to the 9/11 attacks, an inspector found a security guard at a nuclear facility asleep on duty for more than a half-hour, but the incident was not considered a serious problem

[43] Moore, Capelli, and Trzeciak, *The "Big Picture" of Insider IT Sabotage.*

[44] Roger G. Johnston, "Security Maxims," Vulnerability Assessment Team, Argonne National Laboratory, September 2013, http://www.ne.anl.gov/capabilities/vat/pdfs/security_maxims.pdf.

[45] Bunn, "Incentives for Nuclear Security."

because no terrorists were attacking at that moment—raising issues about the security culture of both the operator and the regulator.[46]

The U.S. Department of Energy's nuclear laboratories have been known for widespread violations of security rules since the dawn of the nuclear age; during the Manhattan Project, physicist Richard Feynman was barred from certain facilities for illicitly cracking into safes and violating other rules as pranks to reveal vulnerabilities.[47] (Feynman's tales of incompetence at the lab emphasize another important lesson: do not assume that rules will be implemented intelligently.)

Incentives often drive rule-breaking. Consider, as one example, the case of cheating on security tests at Y-12 (years before the recent intrusion). In January 2004, the U.S. Department of Energy inspector general found that for many years the Wackenhut Corporation, which provided security for the Y-12 National Security Complex in Oak Ridge, Tennessee, had been cheating on its security exercises. These exercises simulated attacks on the nuclear facility, challenging the security guards to repel a mock assault. The security tests were important to the guard force: they could affect the payment the security contractor received and possibly the bonuses that security personnel themselves received. Until 2003, the Wackenhut security force received scores of "outstanding" and a total of $2.2 million in bonuses for their performances on security exercises. It was later revealed that, up to three weeks in advance of the exercises, Wackenhut management told Y-12 security officers which buildings and targets would be attacked, the exact number of adversaries, and the location where a diversion would occur. The protective force thus had ample time to formulate special plans on how to counter the adversary, and they were able to place trucks or other obstacles at advantageous points to be used as barricades and concealment by protective force responders for shooting during the exercises. The Wackenhut management also identified the best prepared protective force personnel and substituted them for less prepared personnel, and officers who would normally relieve other protective force personnel were armed and held in "standby" to participate in an exercise, potentially adding six or seven armed responders who would not normally have been available during a shift. And several participants reported that the defenders had also disabled

[46] U.S. Congress, General Accounting Office, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: GAO, September 2003), 12, http://www.gao.gov/new.items/d03752.pdf.

[47] For Feynman's account, see Richard P. Feynman, *Surely You're Joking, Mr. Feynman! Adventures of a Curious Character* (New York: W.W. Norton, 1985), 137–155. For an account of the broader record (possibly more negative than is justified), see President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington, D.C.: PFIAB, June 1999), http://www.fas.org/sgp/library/pfiab/. This report includes a remarkable listing of previous reports on security weaknesses at the Department of Energy.

the sensors in their laser-tag gear, so in the tests they were essentially invincible: the system would never score them as having been shot.[48]

The lesson here is not that security procedures and personnel-screening rules are routinely violated at nuclear power facilities. They are not. Nor is the lesson that nuclear security exercises like those at Y-12 are not important—quite the opposite.

But rules are not followed universally or strictly, especially when they are in tension with other goals, such as continuing production, meeting deadlines, and maintaining collegial relations among coworkers. And tests are likely to be reliable only when they are independent and uncompromised. Nuclear security managers need to think carefully about the incentives employees face, and work to make sure that the incentives point in the direction of good security performance rather than poor security performance.

One element of getting incentives pointed in the right direction is to do away with unneeded security rules—rules that are overly burdensome or complex and that contribute little to the overall security of the plant. When employees encounter rules they think are senseless, they typically do not comply with them. This can contribute to a broader culture in which people follow security rules only when they find it convenient, and they come to think of security as a problem for "them" and not "us." Every high-security organization has some of these unneeded or overly complex rules, as more rules get added over time in response to each incident that arises. By one estimate, "[i]n any large organization, *at least* 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, or actually undermine security (by wasting energy and resources, by creating cynicism about security, and/or by driving behaviors that were not anticipated)."[49] Organizations should have regular processes to search for such rules and get rid of them.

Lesson #9: Don't Assume that Only Consciously Malicious Insider Actions Matter

Some of the highest consequence threats that security organizations face are from malicious outsiders: for intelligence agencies this means an adversary's spies; for military units, it is enemy forces; for nuclear facilities, it is thieves and saboteurs. Security organizations may therefore focus on preventing attacks or theft by outsiders, and to the degree that they protect against insider threats, they focus on the danger that individuals inside the organization might be recruited by or become sympathetic to a malicious outsider group—hence the attention paid to preventing "penetration" through counterintelligence and personnel screening and monitoring.

[48] U.S. Department of Energy, Office of the Inspector General, *Inspection Report: Protective Force Performance Test Improprieties*, DOE/IG-0636 (Washington, D.C.: DOE, January, 2004); http://energy.gov/ig/downloads/inspection-report-protective-force-performance-test-improprieties-doeig-0636.

[49] Johnston, "Mitigating the Insider Threat (and Other Security Issues)."

Yet this focus ignores the possibility that an insider threat can occur when an individual commits a dangerous act, not out of malicious intent, but for other complex reasons. The official definitions of insider threats in the IAEA guidelines encourage this focus because they emphasize the malicious characteristic of such a threat. The first definition introduced is of the term "adversary," which is described as "any individual performing or attempting to perform a malicious act."[50] The IAEA definition of "insider" builds on this definition of adversary: "The term 'insider' is used to describe an adversary with authorized access to a nuclear facility, a transport operation or sensitive information."[51] Thus, both definitions include a component of malice. The IAEA definition of a threat also implies the presence of malicious intent: "The term 'threat' is used to describe a likely cause of harm to people, damage to property or harm to the environment by an individual or individuals with the motivation, intention and capability to commit a malicious act."[52] But individuals who plausibly had no malicious intent even though they had very faulty, even horrific, judgment have caused serious insider threat incidents.

The October 2001 U.S. anthrax attacks, in which at least five letters containing anthrax spores were mailed to reporters and political figures, provide a dramatic case in point—though one where the errors of judgment were so extreme as to edge into the territory covered by the IAEA's definitions. As a result of these mailings, at least twenty-two victims contracted anthrax, five people died, thirty-five postal facilities were contaminated, and the presence of the anthrax spores was found in seven buildings on Capitol Hill.[53] But it appears that there may have been no real intent to kill or sicken anyone. The best available evidence suggests that Bruce Ivins, a senior scientist at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), mailed the envelopes along with letters declaring "Death to America . . . Allah is Great." Ivins was not, however, sympathetic with al-Qaeda, and it is believed that his main motive was to renew national interest in the threat of anthrax. Ronald Schouten, in the *Harvard Review of Psychiatry*, lists Ivins's motives as "an effort to enhance the profile of his anthrax work, to improve his own standing among colleagues, and to stimulate funding for biodefense by inducing fear in the population and influencing government policy."[54]

[50] International Atomic Energy Agency, "Preventive and Protective Measures against Insider Threats" (Vienna: IAEA, September 2008), http://www-pub.iaea.org/MTCD/publications/PDF/pub1359_web.pdf (accessed May 17, 2013).

[51] Ibid.

[52] Ibid.

[53] U.S. Department of Justice, "Amerithrax Investigative Summary," February 19, 2010, http://www.justice.gov/amerithrax/docs/amx-investigative-summary.pdf (accessed May 17, 2013).

[54] Ronald Schouten, "Terrorism and the Behavioral Sciences," *Harvard Review of Psychiatry* 18 (6) (2010): 370.

Personal motives were certainly mixed up with the national security motive: Ivins had been a major contributor to the development of a controversial anthrax vaccine, and a terrorist anthrax attack had the potential to make his work more relevant, increase the patent-related fees that he was receiving, and impress a woman with whom he worked.[55] In retrospect, Ivins was clearly a sick man with warped judgment and a reckless willingness to risk the lives of others, but he did not intend to kill many people through his anthrax mailings. Had he intended to do so, the likely death toll would have been much larger.

Many other examples of "nonmalicious" but highly misguided insiders could be cited: Wen Ho Lee, who, if his version of events is correct, took highly classified information home as a backup system to make consulting work easier after leaving the Los Alamos Laboratory; Oleg Savchuk, who allegedly placed a virus into the computer control system at the Ignalina Nuclear Power Plant in order to call attention to the need for improved security and to be rewarded for his diligence; or John Deutch, the CIA director who handled highly sensitive classified information on an insecure computer connected to the Internet.[56] Indeed, security problems arising through inadvertence, conflicting incentives, and poor judgment are so pervasive that one U.S. security expert concluded: "The insider threat from careless or complacent employees and contractors exceeds the threat from malicious insiders (though the latter is not negligible).... This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders."[57]

The lesson that should be learned from these incidents is that efforts to prevent insider threats primarily through screening for loyalty or, conversely, monitoring for ties to malicious terrorist or criminal organizations are insufficient. Such methods will not detect or deter individuals who make poor judgments, even radically poor judgments, in the name of a private interest or even in pursuit of a distorted vision of the public good. Nuclear security managers need to focus on the nonmalicious sources of insecurity as well. Building a strong security culture and making good security convenient are two places to start.

[55] U.S. Department of Justice, "Amerithrax Investigative Summary"; David Willman, *The Mirage Man: Bruce Ivins, the Anthrax Attacks, and America's Rush to War* (New York: Bantam, 2011), 190; and Jeanne Guillemin, *American Anthrax* (New York: Times Books, 2011), 131.

[56] Wen Ho Lee and Helen Zia, *My Country Versus Me* (New York: Hyperion, 2001); William Potter and Charles Ferguson, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005), 224; and Central Intelligence Agency Inspector General, *Report of Investigation: Improper Handling of Classified Information by John M. Deutch*, 1998-0028-IG (Washington, D.C.: CIA, February 18, 2000). Lee was indicted for stealing classified nuclear weapons designs to share with China, though this has never been proven to the satisfaction of a court. The judge in the case ultimately apologized to Lee for his treatment.

[57] Johnston, *Security Maxims.*

Lesson #10: Don't Focus Only on Prevention and Miss Opportunities for Mitigation

The IAEA's best practices guide for insider threats clearly recognizes the need to maintain both rigorous prevention programs and serious mitigation preparations as part of any nuclear security program. Indeed, even the title of the guide, *Preventive and Protective Measures against Insider Threats*, highlights that need. Yet there can be a strong temptation to favor prevention efforts over mitigation efforts, especially when dealing with exercises in which the public is involved, in order to avoid public fears that security incidents are likely.

Although the 2011 Fukushima accident is clearly a safety, not security, incident, it highlights the dangers that can be created when operators and officials avoid practicing mitigation and emergency response preparations in order to enhance public support for nuclear power and prevent panic. Yoichi Funabashi and Kay Kitazawa have compellingly identified a dangerous "myth of absolute safety" that was used to promote confidence in accident prevention measures, rather than conduct nuclear emergency response activities in Japan prior to the March 2011 accident. As Funabashi and Kitazawa explain:

> This myth [of absolute safety] has been propagated by interest groups seeking to gain broad acceptance for nuclear power: A public relations effort on behalf of the absolute safety of nuclear power was deemed necessary to overcome the strong anti-nuclear sentiments connected to the atomic bombings of Hiroshima and Nagasaki. . . . One example of the power of the safety myth involves disaster drills. In 2010, the Niigata Prefecture, where the 2007 Chuetsu offshore earthquake temporarily shut down the Kashiwazaki-Kariwa Nuclear Power Plant, made plans to conduct a joint earthquake and nuclear disaster drill. But NISA (the Nuclear and Industrial Safety Agency) advised that a nuclear accident drill premised on an earthquake would cause unnecessary anxiety and misunderstanding among residents. The prefecture instead conducted a joint drill premised on heavy snow.[58]

The myth that the facilities were absolutely safe was repeated so often that it affected operators' thinking about emergency response. The accident response plan for the Fukushima Daiichi site reportedly said, "The possibility of a severe accident occurring is so small that from an engineering standpoint, it is practically unthinkable." If that is what you believe, you are not likely to put much effort into preparing to mitigate severe accidents—and they did not.[59]

Fortunately, important steps can be taken to mitigate both sabotage and theft at nuclear facilities. The key steps to mitigate severe sabotage are largely the same as the key steps to mitigate severe accidents: making sure that electric

[58] Yoichi Funabashi and Kay Kitazawa, "Fukushima in Review: A Complex Disaster, a Disastrous Response," *Bulletin of the Atomic Scientists* 68 (March/April 2012): 13–14.

[59] Phred Dvorak and Peter Landers, "Japanese Plant Had Barebones Risk Plan," *The Wall Street Journal*, March 31, 2011.

power can be rapidly restored, that the reactor core and the fuel in the spent fuel pool can always be kept under water, and that if radioactivity *is* released from the core, the amount released to the environment can be limited.

With respect to nuclear material theft, mitigation steps are less effective, for once nuclear material has left the site where it is supposed to be, it could be anywhere; the subsequent lines of defense are largely variations on looking for a needle in a haystack. Nevertheless, relatively simple steps toward mitigation should not be neglected. In recent years, for example, the U.S. government has been pressing for countries to ship plutonium and HEU in forms that would require some chemical processing before they could be used in a bomb, rather than in pure form. Various elements of the effort to interdict nuclear smuggling can also be thought of as mitigation steps should nuclear theft prevention efforts fail.

But the Fukushima case makes clear that it is important to avoid, in both public presentations and private beliefs, the "myth of absolute security." The belief that a facility is already completely secure is never correct—and will lead to complacency that is the enemy of preparedness for either prevention or mitigation. Prevention of insider threats is a high priority, but leaders and operators should never succumb to the temptation to minimize emergency response and mitigation efforts in order to maintain the illusion that there is nothing to be afraid of.

THE PATH FORWARD

Even this brief comparative look at insider threats illustrates that such threats come in diverse and complex forms, that the individuals involved can have multiple complex motives, and that common, though understandable, organizational imperfections make insider threats a difficult problem to address adequately. Most nuclear organizations appear to underestimate both the scale of the insider threat and the difficulty of addressing it. Serious insider threats may well be rare in nuclear security, but given the scale of the potential consequences, it is crucial to do everything reasonably practical to address them.

The main lesson of all these cases is: do not assume, always assess—and assess (and test) as realistically as possible. Unfortunately, realistic testing of how well insider protections work in practice is very difficult; genuinely realistic tests could compromise safety or put testers at risk, while tests that security personnel and other staff know are taking place do not genuinely test the performance of the system. Nevertheless, nuclear security managers need to establish programs for assessment and testing that are as creative and realistic as practicable—and to reward the employees involved for finding vulnerabilities and proposing ways to fix them, rather than marginalizing people who complain about security vulnerabilities. Ensuring that all operators handling nuclear weapons, weapons-usable nuclear materials, or nuclear facilities whose sabotage could have catastrophic consequences have genuinely effective measures in place to cope with insider threats should be a major focus of the nuclear security summit process, of the

IAEA's nuclear security efforts, of WINS's nuclear security program, and of regulatory and industry efforts around the world.

Complacency—the belief that the threat is modest and the measures already in place are adequate—is the principal enemy of action. Hence, a better understanding of the reality of the threat is critical to getting countries around the world to put stronger protections in place.

To foster such an understanding, we recommend that countries work together to establish shared analyses of incidents and lessons learned. In the world of nuclear safety, when an incident occurs, the plant performs a root-cause analysis and develops lessons learned to prevent similar incidents from occurring again. These incident reports and lessons learned are then shared with other reactor operators through organizations such as WANO and national groups such as the U.S. Institute of Nuclear Power Operations (INPO). These organizations can then assess trends among the incidents. INPO not only distributes lessons learned to U.S. reactor operators, it carries out inspections to assess how well reactor operators are implementing lessons learned. Nothing remotely resembling this approach exists in the nuclear security world. It is time to begin such an effort—assessing security-related incidents in depth, exploring lessons learned, and distributing as much of this information among nuclear security operators as necessary secrecy will allow. As we have done in this paper, the analyses should include non-nuclear incidents that reveal types of problems that arise and types of tactics against which nuclear materials and facilities should be protected. Information about incidents and how to protect against them could be a major driver of nuclear security improvement, as it has been in safety; in a recent survey of nuclear security experts in eighteen countries with weapons-usable nuclear material, incidents were cited far more often than any other factor as a dominant or very important driver of countries' recent changes in nuclear security policies.[60] States could begin with internal assessments of events within their territory, and then provide as much information as possible to an international collection of facts and findings.

Overall, there is a need for more in-depth, empirically grounded research on insider threats to nuclear security and what works best in protecting against them. Such research focused on cybersecurity is beginning to become available, but genuinely empirical work on nuclear security is in its infancy. Fortunately, only a modest number of serious insider cases have been identified in the nuclear world. Unfortunately, it is likely, given the classified nature of security records and reports, that we have not identified all serious cases of insider threats from the past. Moreover, the potential danger is so high in the nuclear world that even a modest number of insider incidents is alarming. There is much research and analysis to be done—and action to be taken. This paper is only a beginning, not an end.

[60] Bunn and Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World*, http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.

Contributors

Matthew Bunn is Professor of Practice at the Harvard Kennedy School. His research interests include nuclear theft and terrorism; nuclear proliferation and measures to control it; the future of nuclear energy and its fuel cycle; and innovation in energy technologies. Before coming to Harvard, he served as an adviser to the White House Office of Science and Technology Policy, as a study director at the National Academy of Sciences, and as editor of *Arms Control Today*. He is the author or coauthor of more than 20 books or major technical reports (most recently *Transforming U.S. Energy Innovation)*, and over a hundred articles in publications ranging from *Science* to *The Washington Post*.

Scott D. Sagan is the Caroline S.G. Munro Professor of Political Science and Senior Fellow at the Center for International Security and Cooperation at Stanford University. He is a Fellow of the American Academy of Arts and Sciences and Cochair of the Academy's Global Nuclear Future Initiative. He is the author of, among other works, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (1993) and *The Spread of Nuclear Weapons: An Enduring Debate* (with Kenneth N. Waltz, 2012).

American Academy of Arts and Sciences

CHERISHING KNOWLEDGE · FOUNDED 1780 · SHAPING THE FUTURE

AMERICAN ACADEMY OF ARTS & SCIENCES

EXHIBIT E

Statement for the Record

Worldwide Threat Assessment
of the
US Intelligence Community

Senate Select Committee on Intelligence

James R. Clapper

Director of National Intelligence

March 12, 2013

Golden-1

US INTELLIGENCE COMMUNITY
WORLDWIDE THREAT ASSESSMENT
STATEMENT FOR THE RECORD

March 12, 2013

INTRODUCTION

Chairman Feinstein, Vice Chairman Chambliss, and Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2013 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom it is my privilege and honor to lead.

This year, in both content and organization, this statement illustrates how quickly and radically the world—and our threat environment—are changing. This environment is demanding reevaluations of the way we do business, expanding our analytic envelope, and altering the vocabulary of intelligence. Threats are more diverse, interconnected, and viral than at any time in history. Attacks, which might involve cyber and financial weapons, can be deniable and unattributable. Destruction can be invisible, latent, and progressive. We now monitor shifts in human geography, climate, disease, and competition for natural resources because they fuel tensions and conflicts. Local events that might seem irrelevant are more likely to affect US national security in accelerated time frames.

In this threat environment, the importance and urgency of intelligence integration cannot be overstated. Our progress cannot stop. The Intelligence Community must continue to promote collaboration among experts in every field, from the political and social sciences to natural sciences, medicine, military issues, and space. Collectors and analysts need vision across disciplines to understand how and why developments—and both state and unaffiliated actors—can spark sudden changes with international implications.

The Intelligence Community is committed every day to providing the nuanced, multidisciplinary intelligence that policymakers, diplomats, warfighters, and international and domestic law enforcement need to protect American lives and America's interests anywhere in the world.

Information as of 7 March 2013 was used in the preparation of this assessment.

Table of Contents

Page

GLOBAL THREATS

REGIONAL THREATS

GLOBAL THREATS

CYBER

We are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of—and interaction with—the world are becoming more intertwined with digital technologies and the Internet. In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks.

State and nonstate actors increasingly exploit the Internet to achieve strategic objectives, while many governments—shaken by the role the Internet has played in political instability and regime change—seek to increase their control over content in cyberspace. The growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation.

Compounding these developments are uncertainty and doubt as we face new and unpredictable cyber threats. In response to the trends and events that happen in cyberspace, the choices we and other actors make in coming years will shape cyberspace for decades to come, with potentially profound implications for US economic and national security.

In the United States, we define cyber threats in terms of **cyber attacks** and **cyber espionage.** A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days. Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information.

Increasing Risk to US Critical Infrastructure

We judge that there is a remote chance of a major cyber attack against US critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage. The level of technical expertise and operational sophistication required for such an attack—including the ability to create physical damage or overcome mitigation factors like manual overrides—will be out of reach for most actors during this time frame. Advanced cyber actors—such as **Russia** and **China**—are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests.

However, isolated state or nonstate actors might deploy less sophisticated cyber attacks as a form of retaliation or provocation. These less advanced but highly motivated actors could access some poorly protected US networks that control core functions, such as power generation, during the next two years, although their ability to leverage that access to cause high-impact, systemic disruptions will probably be limited. At the same time, there is a risk that unsophisticated attacks would have significant outcomes due to unexpected system configurations and mistakes, or that vulnerability at one node might spill over and contaminate other parts of a networked system.

- Within the past year, in a denial-of-service campaign against the public websites of multiple US banks and stock exchanges, actors flooded servers with traffic and prevented some customers from accessing their accounts via the Internet for a limited period, although the attacks did not alter customers' accounts or affect other financial functions.

- In an August 2012 attack against Saudi oil company Aramco, malicious actors rendered more than 30,000 computers on Aramco's business network unusable. The attack did not impair production capabilities.

Eroding US Economic and National Security

Foreign intelligence and security services have penetrated numerous computer networks of US Government, business, academic, and private sector entities. Most detected activity has targeted unclassified networks connected to the Internet, but foreign cyber actors are also targeting classified networks. Importantly, much of the nation's critical proprietary data are on sensitive but unclassified networks; the same is true for most of our closest allies.

- We assess that highly networked business practices and information technology are providing opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive US national security and economic data. This is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena.

- It is very difficult to quantify the value of proprietary technologies and sensitive business information and, therefore, the impact of economic cyber espionage activities. However, we assess that economic cyber espionage will probably allow the actors who take this information to reap unfair gains in some industries.

Information Control and Internet Governance

Online **information control** is a key issue among the United States and other actors. However, some countries, including Russia, China, and Iran, focus on "cyber influence" and the risk that Internet content might contribute to political instability and regime change. The United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems. This is a fundamental difference in how we define cyber threats.

The current multi-stakeholder model of Internet governance provides a forum for governments, the commercial sector, academia, and civil society to deliberate and reach consensus on Internet organization and technical standards. However, a movement to reshape Internet governance toward a national government-based model would contradict many of our policy goals, particularly those to protect freedom of expression and the free flow of online information and ensure a free marketplace for information technology products and services.

- These issues were a core part of the discussions as countries negotiated a global telecommunications treaty in Dubai in December. The contentious new text that resulted led many countries, including the United States, not to sign the treaty because of its language on network security, spam control, and expansion of the UN's role in Internet governance. The negotiations demonstrated that disagreements on these issues will be long-running challenges in bilateral and multilateral engagements.

Internet governance revision based on the state-management model could result in international regulations over online content, restricted exchange of information across borders, substantial slowdown of technical innovation, and increased opportunities for foreign intelligence and surveillance operations on the Internet in the near term.

Other Actors

We track cyber developments among nonstate actors, including terrorist groups, hacktivists, and cyber criminals. We have seen indications that some **terrorist organizations** have heightened interest in developing offensive cyber capabilities, but they will probably be constrained by inherent resource and organizational limitations and competing priorities.

Hacktivists continue to target a wide range of companies and organizations in denial-of-service attacks, but we have not observed a significant change in their capabilities or intentions during the last year. Most hacktivists use short-term denial-of-service operations or expose personally identifiable information held by target companies, as forms of political protest. However, a more radical group might form to inflict more systemic impacts—such as disrupting financial networks—or accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack.

Cybercriminals also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and nonstate actors. In addition, a handful of **commercial companies** sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems.

TERRORISM and TRANSNATIONAL ORGANIZED CRIME

Terrorism

Terrorist threats are in a transition period as the global jihadist movement becomes increasingly decentralized. In addition, the Arab Spring has generated a spike in threats to US interests in the region that likely will endure until political upheaval stabilizes and security forces regain their capabilities. We also face uncertainty about potential threats from Iran and Lebanese Hizballah, which see the United States and Israel as their principal enemies.

Evolving Homeland Threat Landscape

Al-Qa'ida in the Arabian Peninsula (AQAP). Attacks on US soil will remain part of AQAP's transnational strategy; the group continues to adjust its tactics, techniques and procedures for targeting the West. AQAP leaders will have to weigh the priority they give to US plotting against other internal and regional objectives, as well as the extent to which they have individuals who can manage, train, and deploy operatives for US operations.

Al-Qa'ida-Inspired Homegrown Violent Extremists (HVE). Al-Qa'ida-inspired HVEs—whom we assess will continue to be involved in fewer than 10 domestic plots per year—will be motivated to engage in violent action by global jihadist propaganda, including English-language material, such as AQAP's *Inspire* magazine; events in the United States or abroad perceived as threatening to Muslims; the perceived success of other HVE plots, such as the November 2009 attack at Fort Hood, Texas, and the March 2012 attacks by an al-Qa'ida-inspired extremist in Toulouse, France; and their own grievances. HVE planning in 2012 was consistent with tactics and targets seen in previous HVE plots and showed continued interest in improvised explosive devices (IED) and US Department of Defense (DoD) targets.

Core Al-Qa'ida. Senior personnel losses in 2012, amplifying losses and setbacks since 2008, have degraded core al-Qa'ida to a point that the group is probably unable to carry out complex, large-scale attacks in the West. However, the group has held essentially the same strategic goals since its initial public declaration of war against the United States in 1996, and to the extent that the group endures, its leaders will not abandon the aspiration to attack inside the United States.

The Global Jihadist Threat Overseas: Affiliates, Allies, and Sympathizers

In 2011, al-Qa'ida and its affiliates played little or no role in the uprisings in the Middle East and North Africa and, with the exception of AQAP, were not well positioned to take advantage of events. At the same time, the rise of new or transitional governments in Egypt, Tunisia, Yemen, and Libya, and ongoing unrest in Syria and Mali, have offered opportunities for established affiliates, aspiring groups, and like-minded individuals to conduct attacks against US interests. Weakened or diminished counterterrorism capabilities, border control mechanisms, internal security priorities, and other shortcomings in these countries—combined with anti-US grievances or triggering events—will sustain the threats to US interests throughout the region. The dispersed and decentralized nature of the terrorist networks active in the region highlights that the threat to US and Western interests overseas is more likely to be unpredictable. The 2012 attack on the US facilities in Benghazi, Libya, and the 2013 attack on Algeria's In-Amenas oil facility demonstrate the threat to US interests from splinter groups, ad hoc coalitions, or individual terrorists who can conduct anti-US operations, even in the absence of official direction or guidance from leaders of established al-Qa'ida affiliates.

- **Al-Qa'ida in Iraq's (AQI)** goals inside Iraq will almost certainly take precedence over US plotting, but the group will remain committed to al-Qa'ida's global ideology. Since the 2011 withdrawal of US forces, AQI has conducted nearly monthly, simultaneous, coordinated country-wide attacks against government, security, and Shia civilian targets. AQI's Syria-based network, the Nusrah Front, is one of the best organized and most capable of the Sunni terrorist groups.

- Somalia-based **al-Shabaab** will remain focused on local and regional challenges, including its longstanding leadership rivalries and its fights against forces from the Somali and Ethiopian Governments and the African Union Mission in Somalia (AMISOM). The group will probably also continue to plot attacks designed to weaken regional adversaries, including targeting US and Western interests in East Africa.

- **Al-Qa'ida in the Land of the Islamic Maghreb's (AQIM)** intentions and capability remain focused on local, US, and Western interests in north and west Africa.
- Nigeria-based **Boko Haram** will continue to select targets for attacks to destabilize the country and advance its extreme vision of Islamist rule.
- Pakistan-based **Lashkar-e-Tayibba (LT)** will continue to be the most multifaceted and problematic of the Pakistani militant groups. The group has the long-term potential to evolve into a permanent and even HAMAS/Hizballah-like presence in Pakistan.

Iran and Lebanese Hizballah

The failed 2011 plot against the Saudi Ambassador in Washington shows that Iran may be more willing to seize opportunities to attack in the United States in response to perceived offenses against the regime. Iran is also an emerging and increasingly aggressive cyber actor. However, we have not changed our assessment that Iran prefers to avoid direct confrontation with the United States because regime preservation is its top priority.

Hizballah's overseas terrorist activity has been focused on Israel—an example is the Bulgarian Government's announcement that Hizballah was responsible for the July 2012 bus bombing at the Burgas airport that killed five Israeli citizens. We continue to assess that the group maintains a strong anti-US agenda but is reluctant to confront the United States directly outside the Middle East.

Transnational Organized Crime

Transnational organized crime (TOC) networks erode good governance, cripple the rule of law through corruption, hinder economic competitiveness, steal vast amounts of money, and traffic millions of people around the globe. (Cybercrime, an expanding for-profit TOC enterprise, is addressed in the Cyber section.) TOC threatens US national interests in a number of ways:

Drug Activity. Drug trafficking is a major TOC threat to the United States and emanates primarily from the Western Hemisphere. Mexico is the dominant foreign producer of heroin, marijuana, and methamphetamines for the US market. Colombia produces the overwhelming majority of the cocaine that reaches the United States, although the amount of cocaine available to US consumers has substantially decreased in the past five years due to Colombian eradication and security efforts, US transit zone interdiction and capacity-building activities, and warfare among Mexican trafficking organizations. However, high US demand—still twice that of Europe—the capacity of Colombia's remaining drug trafficking organizations, and weak penal and judicial institutions suggest that Colombia's decades-long struggle with the drug threat will continue for a number of years. In addition to the threat inside the United States, the drug trade undermines US interests abroad; for example, it erodes stability in West and North Africa and remains a significant source of revenue for the Taliban in Afghanistan.

Facilitating Terrorist Activity. The Intelligence Community is monitoring the expanding scope and diversity of "facilitation networks," which include semi-legitimate travel experts, attorneys, and other types of professionals, as well as corrupt officials, who provide support services to criminal and terrorist groups.

Money Laundering. The scope of worldwide money laundering is subject to significant uncertainty but measures more than a trillion dollars annually, often exploiting governments' difficulties coordinating law enforcement across national boundaries. Criminals' reliance on the US dollar also exposes the US financial system to illicit financial flows. Inadequate anti-money laundering regulations, lax enforcement of existing ones, misuse of front companies to obscure those responsible for illicit flows, and new forms of electronic money challenge international law enforcement efforts.

Corruption. Corruption exists at some level in all countries; however, the interaction between government officials and TOC networks is particularly pernicious in some countries. Among numerous examples, we assess that Guinea-Bissau has become a narco-state, where traffickers use the country as a transit hub with impunity; and in Russia, the nexus among organized crime, some state officials, the intelligence services, and business blurs the distinction between state policy and private gain.

Human Trafficking. President Obama recently noted that upwards of 20 million human beings are being trafficked around the world. The US State Department and our law enforcement organizations have led US Government efforts against human trafficking, and the Intelligence Community has increased collection and analytic efforts to support law enforcement and the interagency Human Smuggling and Trafficking Center. Virtually every country in the world is a source, transit point, and/or destination for individuals being trafficked.

- For example, in 2012 a Ukrainian National was sentenced to life-plus-20-years in prison for operating a human trafficking organization that smuggled young Ukrainians into the United States. For seven years, he and his brothers arranged to move unsuspecting immigrants through Mexico into the United States. With debts of $10,000 to $50,000, victims were forced to live in squalid conditions, enslaved, and subjected to rape, beatings, and other forms of physical attack. Threats against their families in Ukraine were used to dissuade them from attempting to escape.

Environmental Crime. Illicit trade in wildlife, timber, and marine resources constitutes a multi-billion dollar industry annually, endangers the environment, and threatens to disrupt the rule of law in important countries around the world. These criminal activities are often part of larger illicit trade networks linking disparate actors—from government and military personnel to members of insurgent groups and transnational organized crime organizations.

WMD PROLIFERATION

Nation-state efforts to develop or acquire weapons of mass destruction (WMD) and their delivery systems constitute a major threat to the security of our nation, deployed troops, and allies. The Intelligence Community is focused on the threat and destabilizing effects of nuclear proliferation, proliferation of chemical and biological warfare (CBW)-related materials, and development of WMD delivery systems.

Traditionally, international agreements and diplomacy have deterred most nation-states from acquiring biological, chemical, or nuclear weapons, but these constraints may be of less utility in preventing terrorist groups from doing so. The time when only a few states had access to the most dangerous technologies is past. Biological and chemical materials and technologies, almost always dual-use, move easily in our globalized economy, as do the personnel with scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse globally and rapidly.

Golden-10

Iran and North Korea Developing WMD-Applicable Capabilities

We assess **Iran** is developing nuclear capabilities to enhance its security, prestige, and regional influence and give it the ability to develop nuclear weapons, should a decision be made to do so. We do not know if Iran will eventually decide to build nuclear weapons.

Tehran has developed technical expertise in a number of areas—including uranium enrichment, nuclear reactors, and ballistic missiles—from which it could draw if it decided to build missile-deliverable nuclear weapons. These technical advancements strengthen our assessment that Iran has the scientific, technical, and industrial capacity to eventually produce nuclear weapons. This makes the central issue its political will to do so.

Of particular note, Iran has made progress during the past year that better positions it to produce weapons-grade uranium (WGU) using its declared facilities and uranium stockpiles, should it choose to do so. Despite this progress, we assess Iran could not divert safeguarded material and produce a weapon-worth of WGU before this activity is discovered.

We judge Iran's nuclear decisionmaking is guided by a cost-benefit approach, which offers the international community opportunities to influence Tehran. Iranian leaders undoubtedly consider Iran's security, prestige and influence, as well as the international political and security environment, when making decisions about its nuclear program. In this context, we judge that Iran is trying to balance conflicting objectives. It wants to advance its nuclear and missile capabilities and avoid severe repercussions—such as a military strike or regime threatening sanctions.

We judge Iran would likely choose a ballistic missile as its preferred method of delivering a nuclear weapon, if one is ever fielded. Iran's ballistic missiles are capable of delivering WMD. In addition, Iran has demonstrated an ability to launch small satellites, and we grow increasingly concerned that these technical steps—along with a regime hostile toward the United States and our allies—provide Tehran with the means and motivation to develop larger space-launch vehicles and longer-range missiles, including an intercontinental ballistic missile (ICBM).

Iran already has the largest inventory of ballistic missiles in the Middle East, and it is expanding the scale, reach, and sophistication of its ballistic missile arsenal. Iran's growing ballistic missile inventory and its domestic production of anti-ship cruise missiles (ASCM) and development of its first long-range land attack cruise missile provide capabilities to enhance its power projection. Tehran views its conventionally armed missiles as an integral part of its strategy to deter—and if necessary retaliate against—forces in the region, including US forces.

North Korea's nuclear weapons and missile programs pose a serious threat to the United States and to the security environment in East Asia, a region with some of the world's largest populations, militaries, and economies. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria's construction of a nuclear reactor, destroyed in 2007, illustrate the reach of its proliferation activities. Despite the Six-Party Joint Statements issued in 2005 and 2007, in which North Korea reaffirmed its commitment not to transfer nuclear materials, technology, or know-how, we remain alert to the possibility that North Korea might again export nuclear technology.

North Korea announced on 12 February that it conducted its third nuclear test. It has also displayed what appears to be a road-mobile ICBM and in December 2012 placed a satellite in orbit using its Taepo Dong 2 launch vehicle. These programs demonstrate North Korea's commitment to develop long-range missile technology that could pose a direct threat to the United States, and its efforts to produce and market ballistic missiles raise broader regional and global security concerns.

Because of deficiencies in their conventional military forces, North Korean leaders are focused on deterrence and defense. The Intelligence Community has long assessed that, in Pyongyang's view, its nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy. We do not know Pyongyang's nuclear doctrine or employment concepts. Although we assess with low confidence that the North would only attempt to use nuclear weapons against US forces or allies to preserve the Kim regime, we do not know what would constitute, from the North's perspective, crossing that threshold.

WMD Security in Syria

We assess **Syria** has a highly active chemical warfare (CW) program and maintains a stockpile of sulfur mustard, sarin, and VX. We assess that Syria has a stockpile of munitions—including missiles, aerial bombs, and possibly artillery rockets—that can be used to deliver CW agents. Syria's overall CW program is large, complex, and geographically dispersed, with sites for storage, production, and preparation. This advanced CW program has the potential to inflict mass casualties, and we assess that an increasingly beleaguered regime, having found its escalation of violence through conventional means inadequate, might be prepared to use CW against the Syrian people. In addition, groups or individuals in Syria could gain access to CW-related materials. The United States and our allies are monitoring Syria's chemical weapons stockpile.

Based on the duration of Syria's longstanding biological warfare (BW) program, we judge that some elements of the program may have advanced beyond the research and development stage and may be capable of limited agent production. Syria is not known to have successfully weaponized biological agents in an effective delivery system, but it possesses conventional and chemical weapon systems that could be modified for biological agent delivery.

COUNTERINTELLIGENCE

Foreign intelligence services, along with terrorist groups, transnational criminal organizations, and other nonstate actors, are targeting and acquiring our national security information, undermining our economic and technological advantages, and seeking to influence our national policies and processes covertly. These foreign intelligence efforts employ traditional methods of espionage and, with growing frequency, innovative technical means. Among significant foreign threats, **Russia** and **China** remain the most capable and persistent intelligence threats and are aggressive practitioners of economic espionage against the United States. Countering such foreign intelligence threats is a top priority for the Intelligence Community for the year ahead. Moreover, vulnerabilities in global supply chains open opportunities for adversaries to exploit US critical infrastructure. (For a discussion of cyber espionage, see the Cyber section.)

Threats to US Government Supply Chains

The US and other national economies have grown more dependent on global networks of supply chains. These web-like relationships, based on contracts and subcontracts for component parts, services, and manufacturing, obscure transparency into those supply chains. Additionally, reliance on foreign equipment, combined with a contracting pool of suppliers in the information technology, telecommunications, and energy sectors, creates opportunities for exploitation of, and increased impact on, US critical infrastructures and systems.

Interdependence of information technologies and integration of foreign technology in US information technology, telecommunications, and energy sectors will increase the potential scope and impact of foreign intelligence and security services' supply chain operations. The likely continued consolidation of infrastructure suppliers—which means that critical infrastructures and networks will be built from a more limited set of provider and equipment options—will also increase the scope and impact of potential supply chain subversions.

COUNTERSPACE

Space systems and their supporting infrastructures enable a wide range of services, including communication; position, navigation, and timing; intelligence, surveillance, and reconnaissance; and meteorology, which provide vital national, military, civil, scientific, and economic benefits. Other nations recognize these benefits to the United States and seek to counter the US strategic advantage by pursuing capabilities to deny or destroy our access to space services. Threats to vital US space services will increase during the next decade as disruptive and destructive counterspace capabilities are developed. In 2007, China conducted a destructive antisatellite test. In a 2009 press article, a senior Russian military leader stated that Moscow was developing counterspace capabilities.

NATURAL RESOURCES: INSECURITY and COMPETITION

Competition and scarcity involving natural resources—food, water, minerals, and energy—are growing security threats. Many countries important to the United States are vulnerable to natural resource shocks that degrade economic development, frustrate attempts to democratize, raise the risk of regime-threatening instability, and aggravate regional tensions. Extreme weather events (floods, droughts, heat waves) will increasingly disrupt food and energy markets, exacerbating state weakness, forcing human migrations, and triggering riots, civil disobedience, and vandalism. Criminal or terrorist elements can exploit any of these weaknesses to conduct illicit activity and/or recruitment and training. Social disruptions are magnified in growing urban areas where information technology transmits grievances to larger—often youthful and unemployed—audiences, and relatively "small" events can generate significant effects across regions or the world.

Food

Natural food-supply disruptions, due to floods, droughts, heat waves, and diseases, as well as policy choices, probably will stress the global food system in the immediate term, resulting in sustained volatility in global food prices. Policy choices can include export bans; diversions of arable lands for other uses, such as urban development; and foreign land leases and acquisitions. Many resource-strapped countries have been losing confidence in the global marketplace to supply vital resources, and increasingly looking to shield their populations in ways that will almost certainly threaten global food production. For example, emerging powers and Gulf States are buying up arable and grazing land around the world as hedges against growing domestic demand and strained resources. Food supplies are also at risk from plant diseases that affect grain and oilseed crops and from transmittable animal diseases, such as H5N1 and foot and mouth disease. At the same time, agricultural inputs—water, fertilizer, land, and fuel oil—are becoming more scarce and/or costly, exacerbating the upward pressure on food prices.

In the coming year, markets for agricultural commodities will remain tight, due in part to drought and crop failures in the midwestern United States last summer. Rising demand for biofuels and animal feed exerts particular pressures on corn prices, and extreme weather will cause episodic deficits in production. We will also see growing demand and high price volatility for wheat. Significant wheat production occurs in water-stressed and climate-vulnerable regions in Asia, where markets will remain susceptible to harvest shocks. A near-term supply disruption could result when a plant disease known as Ug99 stem rust—already spreading across Africa, Asia, and the Middle East—arrives in South Asia, which is likely to happen within the next few years. Wheat production is growing in Eastern Europe, but output is variable, and governments have demonstrated a readiness to impose export controls.

Although food-related state-on-state conflict is unlikely in the near term, the risk of conflict between farmers and livestock owners—often in separate states—will increase as population growth and crop expansion infringe on livestock grazing areas, especially in sub-Saharan Africa and Central Asia. Disputes over fisheries are also likely to increase as water scarcity emerges in major river basins, and marine fisheries are depleted. Shrinking marine fisheries—for example, in the South China Sea—will lead to diplomatic disputes as fishermen are forced to travel further from shore. In addition, government grants of state-owned land to domestic and foreign agricultural developers are likely to stoke conflict in areas without well-defined land ownership laws and regulations.

Terrorists, militants, and international crime organizations can use declining local food security to promote their own legitimacy and undermine government authority. Growing food insecurity in weakly governed countries could lead to political violence and provide opportunities for existing insurgent groups to capitalize on poor conditions, exploit international food aid, and discredit governments for their inability to address basic needs. In addition, intentional introduction of a livestock or plant disease might be a greater threat to the United States and the global food system than a direct attack on food supplies intended to kill humans.

Water

Risks to freshwater supplies—due to shortages, poor quality, floods, and climate change—are growing. These forces will hinder the ability of key countries to produce food and generate energy, potentially undermining global food markets and hobbling economic growth. As a result of demographic and economic development pressures, North Africa, the Middle East, and South Asia face particular difficulty coping with water problems.

Lack of adequate water is a destabilizing factor in countries that do not have the management mechanisms, financial resources, or technical ability to solve their internal water problems. Some states are further stressed by heavy dependence on river water controlled by upstream nations with unresolved water-sharing issues. Wealthier developing countries probably will experience increasing water-related social disruptions, although they are capable of addressing water problems without risk of state failure.

Historically, water tensions have led to more water-sharing agreements than violent conflicts. However, where water-sharing agreements are ignored, or when infrastructure development—for electric power generation or agriculture—is seen as a threat to water resources, states tend to exert leverage over their neighbors to preserve their water interests. This leverage has been applied in international forums and has included pressuring investors, nongovernmental organizations, and donor countries to support or halt water infrastructure projects. In addition, some nonstate terrorists or extremists will almost certainly target vulnerable water infrastructure to achieve their objectives and continue to use water-related grievances as recruitment and fundraising tools.

Many countries are using groundwater faster than aquifers can replenish in order to satisfy food demand. In the long term, without mitigation actions (drip irrigation, reduction of distortive electricity-for-water pump subsidies, access to new agricultural technology, and better food distribution networks), exhaustion of groundwater sources will cause food demand to be satisfied through increasingly stressed global markets.

Water shortages and pollution will also harm the economic performance of important US trading partners. Economic output will suffer if countries do not have sufficient clean water to generate electrical power or to maintain and expand manufacturing and resource extraction. In some countries, water shortages are already having an impact on power generation, and frequent droughts are undermining long-term plans to increase hydropower capacity. With climate change, these conditions will continue to deteriorate.

Minerals: China's Monopoly on Rare Earth Elements

Rare earth elements (REE) are essential to civilian and military technologies and to the 21st century global economy, including development of green technologies and advanced defense systems. China holds a commanding monopoly over world REE supplies, controlling about 95 percent of mined production and refining. China's dominance and policies on pricing and exports are leading other countries to pursue mitigation strategies, but those strategies probably will have only limited impact within the next five years and will almost certainly not end Chinese REE dominance. REE prices spiked after China enacted a 40-percent export quota cut in July 2010, peaking at record highs in mid-2011. As of December 2012, REE prices had receded but still remained at least 80 percent, and as much as 600 percent (depending on the type of REE), above pre-July 2010 levels.

Mines in Australia, Brazil, Canada, Malawi, the United States, and Vietnam are expected to be operational in less than five years. However, even as production at non-Chinese mines come online, initial REE processing outside of China will remain limited because of technical difficulties, regulatory hurdles, and capital costs associated with the startup of new or dormant processing capabilities and facilities. China will also continue to dominate production of the most scarce and expensive REEs, known as heavy REEs, which are critical to defense systems.

Energy

Oil prices will remain highly sensitive to political instability in the Middle East, tensions with Iran, and global economic growth. In 2012 increasing US, Iraqi, and Libyan output, combined with slow economic growth, helped ease upward pressure on prices. In the coming year, most growth in new production probably will come from North America and Iraq, while production from some major producers stagnates or declines because of policies that discourage investment.

Sustained oil prices above $80 per barrel would support the growth in North American oil production. That growth is being propelled by the production of tight oil, due to the application of horizontal drilling and hydrolic fracturing. Many Organization of the Petroleum Exporting Countries (OPEC) members are increasingly dependent on high oil prices to support government spending. However, the budgets of countries that subsidize domestic fuel consumption will come under greater stress with high oil prices and rising domestic demand.

Natural gas prices will remain regionally based, with North American consumers probably paying one-third the price of European importers and one-fourth that of Asian consumers. With the prospects for US liquefied natural gas (LNG) exports made possible by the growth in shale gas production, along with other global LNG exports, major European and Asian importers probably will continue to pressure their suppliers to de-link their prices from oil. Weather, economic indicators, and energy policies in Japan probably will have the strongest influence on global LNG prices. Australia is poised to become a top LNG exporter but faces project cost inflation that could slow development.

Climate Change and Demographics

Food security has been aggravated partly because the world's land masses are being affected by weather conditions outside of historical norms, including more frequent and extreme floods, droughts, wildfires, tornadoes, coastal high water, and heat waves. Rising temperature, for example, although enhanced in the Arctic, is not solely a high-latitude phenomenon. Recent scientific work shows that temperature anomalies during growing seasons and persistent droughts have hampered agricultural productivity and extended wildfire seasons. Persistent droughts during the past decade have also diminished flows in the Nile, Tigris-Euphrates, Niger, Amazon, and Mekong river basins.

Demographic trends will also aggravate the medium- to long-term outlooks for resources and energy. Through roughly 2030, the global population is expected to rise from 7.1 billion to about 8.3 billion; the size of the world's population in the middle class will expand from the current 1 billion to more than 2 billion; and the proportion of the world's population in urban areas will grow from 50 percent to about 60 percent—all putting intense pressure on food, water, minerals, and energy.

HEALTH and PANDEMIC THREATS

Scientists continue to discover previously unknown pathogens in humans that made the "jump" from animals—zoonotic diseases. Examples are: a prion disease in cattle that jumped in the 1980s to cause variant Creutzeldt-Jacob disease; a bat henipavirus that in 1999 became known as the human Nipah Virus; a bat corona virus that jumped to humans in 2002 to cause Severe Acute Respiratory Syndrome (SARS); and another SARS-like corona virus recently identified in individuals who have been in Saudi

Golden-16

Arabia, which might also have bat origins. Human and livestock population growth and encroachment into jungles increase human exposure to crossovers. No one can predict which pathogen will be the next to spread to humans, or when or where such a development will occur, but humans will continue to be vulnerable to pandemics, most of which will probably originate in animals.

An easily transmissible, novel respiratory pathogen that kills or incapacitates more than one percent of its victims is among the most disruptive events possible. Such an outbreak would result in a global pandemic that causes suffering and death in every corner of the world, probably in fewer than six months. This is not a hypothetical threat. History is replete with examples of pathogens sweeping populations that lack immunity, causing political and economic upheaval, and influencing the outcomes of wars—for example, the 1918 Spanish flu pandemic affected military operations during World War I and caused global economic disruptions.

The World Health Organization has described one influenza pandemic as "the epidemiological equivalent of a flash flood." However, slow-spreading pathogens, such as HIV/AIDS, have been just as deadly, if not more so. Such a pathogen with pandemic potential may have already jumped to humans somewhere; HIV/AIDS entered the human population more than 50 years before it was recognized and identified. In addition, targeted therapeutics and vaccines might be inadequate to keep up with the size and speed of the threat, and drug-resistant forms of diseases, such as tuberculosis, gonorrhea, and Staphylococcus aureus, have already emerged.

MASS ATROCITIES

Mass atrocities continue to be a recurring feature of the global landscape. Most of the time they occur in the context of major instability events. Since the turn of the last century, hundreds of thousands of civilians have lost their lives as a result of atrocities occurring during conflicts in the Darfur region of Sudan and in the eastern Congo (Kinshasa). Recent atrocities in Syria, where tens of thousands of civilians have lost their lives within the past two years, have occurred against a backdrop of major political upheaval, illustrating how most mass atrocities tend to be perpetrated by ruling elites or rebels who use violence against civilians to assert or retain control. Consistent with this trend, mass atrocities also are more likely in places where governments discriminate against minorities, socioeconomic conditions are poor, or local powerbrokers operate with impunity. In addition, terrorists and insurgents might exploit such conditions to conduct attacks against civilians, as in Boko Haram's attacks on churches in Nigeria. Less frequently, violence between sectarian or ethnic groups can create the conditions for mass atrocities.

REGIONAL THREATS

MIDDLE EAST and NORTH AFRICA

Arab Spring

Although some countries have made progress towards democratic rule, most are experiencing uncertainty, violence, and political backsliding. The toppling of leaders and weakening of regimes have also unleashed destabilizing ethnic and sectarian rivalries. Islamist actors have been the chief electoral beneficiaries of the political openings, and Islamist parties in Egypt, Tunisia and Morocco will likely solidify their influence in the coming year. The success of transitioning states will depend, in part, on their ability to integrate these actors into national politics and to integrate—or marginalize—political, military, tribal, and business groups that were part of or benefitted from the old regimes. At the same time, transitions that fail to address public demands for change are likely to revive unrest and heighten the appeal of authoritarian or extremist solutions.

Three issues, in particular, will affect US interests:

- ***Ungoverned Spaces.*** The struggles of new governments in places like Tripoli and Sanaa to extend their writs, as well as the worsening internal conflict in Syria, have created opportunities for extremist groups to find ungoverned space from which to destabilize the new governments and prepare attacks against Western interests inside those countries.

- ***Economic Hardships.*** Many states face economic distress—specifically, high rates of unemployment—that is unlikely to be alleviated by current levels of Western aid and will require assistance from wealthy Arab countries as well as reforms and pro-growth policies. Failure to meet heightened popular expectations for economic improvement could set back transitions in places such as Egypt and destabilize vulnerable regimes such as Jordan. Gulf states provide assistance only incrementally and are wary of new governments' foreign policies and their ability to absorb funds.

- ***Negative Views of the United States.*** Some transitioning governments are more skeptical than their predecessors about cooperating with the United States and are concerned about protecting sovereignty and resisting foreign interference. This has the potential to hamper US counterterrorism efforts and other initiatives to engage transitioning governments.

Egypt

Since his election in June 2012, Egyptian President Muhammad Mursi has worked to consolidate control of the instruments of state power and loosen the Egyptian military's grip on the government. Mursi has taken actions that have advanced his party's agenda and his international reputation, including his late-2012 role brokering a HAMAS-Israeli cease-fire. However, his decree in November 2012 that temporarily increased his authorities at the expense of the judiciary angered large numbers of Egyptians—especially secular activists—and brought protesters back to the streets.

Quelling popular dissatisfaction and building popular support for his administration and policies are critical for Mursi and will have a direct bearing on the Freedom and Justice Party's success in upcoming parliamentary elections. A key element of Mursi's ability to build support will be improving living standards and the economy; GDP growth fell to 1.5 percent in 2012 from just over 5 percent in 2010, and unemployment was roughly 12.6 percent in mid-2012.

Syria

Almost two years into the unrest in Syria, we assess that the erosion of the Syrian regime's capabilities is accelerating. Although the Asad regime has prevented insurgents from seizing key cities—such as Damascus, Aleppo, and Homs—it has been unable to dislodge them from these areas. Insurgent forces also have been gaining strength in rural areas of northern and eastern Syria, particularly Idlib Province along the border with Turkey, where their progress could lead to a more permanent base for insurgent operations. Prolonged instability is also allowing al-Qa'ida's Nusrah Front to establish a presence within Syria. (For details on Syria's weapons and chemical and biological warfare programs, see the Proliferation section.)

- Sanctions and violence have stifled trade, commercial activity, and foreign investment, and reduced the regime's financial resources—as many as 2.5 million people are internally displaced and roughly 700,000 have fled to neighboring countries since March 2011. The Syrian economy contracted by 10 to 15 percent in 2012, which has forced the regime to prioritize security spending and cut back on providing basic services, food and fuel, and health and education services for the public.

Iran

Iran is growing more autocratic at home and more assertive abroad as it faces elite and popular grievances, a deteriorating economy, and an uncertain regional dynamic. Supreme Leader Khamenei's power and authority are now virtually unchecked, and security institutions, particularly the Islamic Revolutionary Guard Corps (IRGC), have greater influence at the expense of popularly elected and clerical institutions. Khamenei and his allies will have to weigh carefully their desire to control the 14 June Iranian presidential election, while boosting voter turnout to increase the appearance of regime legitimacy and avoid a repeat of the disputed 2009 election. Meanwhile, the regime is adopting more oppressive social policies to increase its control over the population, such as further limiting educational and career choices for women.

Iran's financial outlook has worsened since the 2012 implementation of sanctions on its oil exports and Central Bank. Iran's economy contracted in 2012 for the first time in more than two decades. Iran's access to foreign exchange reserves held overseas has diminished, and preliminary data suggest that it suffered its first trade deficit in 14 years. Meanwhile, the rial reached an all-time low in late January, with the exchange rate falling from about 15,000 rials per dollar at the beginning of 2012 to nearly 40,000 rials per dollar, and inflation and unemployment are growing.

Growing public frustration with the government's socioeconomic policies has not led to widespread political unrest because of Iranians' pervasive fear of the security services and the lack of effective opposition organization and leadership. To buoy the regime's popularity and forestall widespread civil unrest, Iranian leaders are trying to soften the economic hardships on the poorer segments of the population. Khamenei has publicly called on the population to pursue a "resistance economy," reminiscent of the hardships that Iran suffered immediately after the Iranian Revolution and during the Iran-Iraq war. However, the willingness of contemporary Iranians to withstand additional economic austerity is unclear because most Iranians do not remember those times; 60 percent of the population was born after 1980 and 40 percent after 1988.

In its efforts to spread influence abroad and undermine the United States and our allies, Iran is trying to exploit the fighting and unrest in the Arab world. It supports surrogates, including Palestinian militants engaged in the recent conflict with Israel. To take advantage of the US withdrawals from Iraq and Afghanistan, it will continue efforts to strengthen political and economic ties with central and local governments, while providing select militants with lethal assistance. Iran's efforts to secure regional hegemony, however, have achieved limited results, and the fall of the Asad regime in Syria would be a major strategic loss for Tehran. (For details on Iran's weapons programs, see the Proliferation section.)

Iraq

Since the US departure, the Iraqi Government has remained generally stable, with the major parties pursuing change through the political process rather than violence. However, there are rising tensions between Prime Minister Maliki and Kurdistan Regional Government President Masud Barzani and an increase in anti-regime Sunni protests since the end of 2012. Maliki is pressing for greater authority over disputed territories in northern Iraq, and Barzani is pushing forward to export hydrocarbons independent of Baghdad.

AQI conducted more vehicle and suicide bombings in 2012 than in 2011, almost exclusively against Iraqi targets. However, AQI and other insurgent groups almost certainly lack sufficient strength to overwhelm Iraqi Security Forces, which has put pressure on these groups through arrests of key individuals.

Iraq is producing and exporting oil at the highest levels in two decades, bolstering finances for a government that derives 90 to 95 percent of its revenue from oil exports. Iraq increased production capacity from about 2.4 million barrels per day in 2010 to roughly 3.3 million barrels per day in 2012. However, it is still wrestling with the challenges of diversifying its economy and providing essential services.

Yemen

We judge that Yemen's new president, Abd Rabuh Mansur Hadi, has diminished the power of former President Salih and his family and kept the political transition on track, but Salih's lingering influence, AQAP's presence, and the tenuous economy are significant challenges. Yemen's humanitarian situation is dire, with nearly half of the population considered "food insecure." Obtaining foreign aid and keeping its oil pipeline open will be crucial to Sanaa's potential economic improvement. The next key political milestone will be the successful completion of an inclusive National Dialogue that keeps Yemen on course for elections in 2014, although some southern leaders are threatening non-participation. Hadi's government will also have to maintain pressure on AQAP following a military offensive this past summer that displaced the group from its southern strongholds.

Lebanon

Lebanon's stability will remain fragile during the next year primarily because of the tensions triggered by the Syrian conflict. We expect Lebanon will be able to avoid destabilizing sectarian violence, but it is likely to experience occasional, localized clashes between pro- and anti-Asad sectarian militias. Thus far, political leaders have succeeded in muting popular outrage over the October 2012 bombing that killed a popular Sunni figure, and the Lebanese Armed Forces remain effective at controlling small-scale violence.

Libya

Libya's leaders are struggling to rebuild after the revolution and the collapse of the Qadhafi regime. The institutional vacuum caused by Qadhafi's removal increased terrorist activity and gave rise to hundreds of well-armed regional militias, many of which played key roles in overthrowing the regime but now complicate Libya's stability. The transitional government is struggling to control the militias, but it remains reliant on some to provide security in the absence of cohesive and capable security institutions. Eastern Libya has been traditional hubs of extremists, and if left unchecked by Libyan authorities and allied militias, groups operating from there could pose a recurring threat to Western interests.

The government is also working to rebuild its administrative capacity as it manages the post-revolutionary transition and is overseeing the drafting of a constitution, which will set the stage for elections as soon as this year. Libya has quickly resumed high levels of oil production, which is critical to rebuilding the economy. As of late 2012, it restored crude oil output to near preconflict levels of 1.6 million barrels per day, but Tripoli will need the expertise and support of international oil companies to sustain, if not boost, overall supply.

SOUTH ASIA

Afghanistan

The upcoming presidential election is scheduled for April 2014, while the International Security Assistance Force (ISAF) is completing its drawdown.

We assess that the Taliban-led insurgency has diminished in some areas of Afghanistan but remains resilient and capable of challenging US and international goals. Taliban senior leaders also continue to be based in Pakistan, which allows them to provide strategic guidance to the insurgency without fear for their safety. Al-Qa'ida's influence on the insurgency is limited, although its propaganda gains from participating in insurgent attacks far outweigh its actual battlefield impact.

Security gains are especially fragile in areas where ISAF surge forces have been concentrated since 2010 and are now transitioning the security lead to Afghan National Security Forces (ANSF). The ANSF will require international assistance through 2014 and beyond. The Afghan National Army and Afghan National Police have proven capable of providing security in major cities, nearby rural areas, and key ground lines of communication in the vicinity of government-controlled areas. The Afghan Air Force has made very little progress. The National Directorate of Security remains Afghanistan's premier national intelligence service and likely will play a larger role in regime security over time.

In addition, Afghanistan's economy, which has been expanding at a steady rate, is likely to slow after 2014. Kabul has little hope of offsetting the coming drop in Western aid and military spending, which have fueled growth in the construction and services sectors. Its licit agricultural sector and small businesses have also benefited from development projects and assistance from nongovernmental organizations, but the country faces high rates of poverty, unemployment, food insecurity, and poppy cultivation.

Pakistan

Pakistan is preparing for national and provincial assembly elections, which must be held no later than May 2013, and a presidential election later in the year. Pakistani officials note that these elections are a milestone—the first time a civilian government has completed a five-year term and conducted a transfer to a new government through the electoral process.

Islamabad is intently focused on Afghanistan in anticipation of the ISAF drawdown. The Pakistani Government has attempted to improve relations with Kabul and ensure that its views are taken into consideration during the transition period. The military this year continued operations in the Federally Administered Tribal Areas (FATA) and, as of late 2012, had forces in place for an operation against anti-Pakistan militants in the North Waziristan Agency of the FATA. There were fewer domestic attacks by the Tehrik-eTaliban Pakistan this year than in the previous several years.

Economically, trouble looms. Pakistan, with its small tax base, poor system of tax collection, and reliance on foreign aid, faces no real prospects for sustainable economic growth. The government has been unwilling to address economic problems that continue to constrain economic growth. The government has made no real effort to persuade its disparate coalition members to accept much-needed policy and tax reforms, because members are focused on retaining their seats in upcoming elections. Sustained remittances from overseas Pakistanis (roughly $13 billion from July 2011 to June 2012, according to Pakistan's central bank) have helped to slow the loss of reserves. However, Pakistan has to repay the IMF $1.7 billion for the rest of this fiscal year for money borrowed as part of its 2008 bailout agreement; growth was around 3.5 percent in 2012; and foreign direct investment and domestic investment have both declined substantially.

India

Both India and Pakistan have made calculated decisions to improve ties, despite deep-rooted mistrust. They held a series of meetings in the past year and will probably continue to achieve incremental progress on economic relations, such as trade, while deferring serious discussion on the more contentious issues of territorial disputes and terrorism. Even modest progress, however, could easily be undone by a terrorist attack against India linked to Pakistan, which could trigger a new crisis and prompt New Delhi to freeze bilateral dialogue.

India will continue to support the current Afghan Government to ensure a stable and friendly Afghanistan. India furthered its engagement with Afghanistan in 2012 and signed an additional four memoranda of understanding on mining, youth affairs, small development projects, and fertilizers during President Karzai's visit to New Delhi in November 2012. We judge that India sees its goals in Afghanistan as consistent with US objectives, and favors sustained ISAF and US presence in the country. India will almost certainly cooperate with the United States and Afghanistan in bilateral and multilateral frameworks to identify assistance activities that will help bolster civil society, develop capacity, and strengthen political structures in Afghanistan. Moreover, India consistently ranks in the top three nations that Afghans see as helping their country rebuild. As of April 2012, India ranked as Afghanistan's fifth largest bilateral donor.

Golden-22

Neither India nor China currently seeks to overturn the strategic balance on the border or commit provocations that would destabilize the relationship. However, India and China are each increasing their military abilities to respond to a border crisis. Both consider these moves to be defensive, but they are probably fueling mutual suspicion and raising the stakes in a potential crisis. As a result, periodic, low-level intrusions between forces along the border could escalate if either side saw political benefit in more forcefully and publicly asserting its territorial claims or responding more decisively to perceived aggression. However, existing mechanisms, as well as a shared desire for stability by political and military leaders from both sides, will likely act as an effective break against escalation.

AFRICA

Throughout Africa, violence, corruption, and extremism pose challenges to US interests in 2013. As in 2012, Africa's stability will be threatened not only by unresolved discord between Sudan and South Sudan, fighting in Somalia, and extremist attacks in Nigeria, but also by the collapse of governance in northern Mali and renewed conflict in the Great Lakes region. Elsewhere, African countries are vulnerable to political crises, democratic backsliding, and natural disasters. On the positive side, in parts of the continent, development is advancing—for example, in Ghana—and, in Somalia, international efforts and domestic support are widening areas of tenuous stability.

Sudan and South Sudan

Sudan's President Bashir and the National Congress Party (NCP) are confronting a range of challenges, including public dissatisfaction over economic decline and insurgencies on Sudan's southern and western borders. Sudanese economic conditions have deteriorated since South Sudan's independence, when South Sudan took control of the majority of oil reserves. The country now faces a decline in economic growth that jeopardizes political stability and fuels opposition to Bashir and the NCP. Khartoum is likely to resort to heavy-handed tactics to prevent protests from escalating and will pursue a military response to provocations by Sudan People's Liberation Movement-North (SPLM-N) rebels in Southern Kordofan and Blue Nile States. An uptick in violence in Sudan's western Darfur region toward the end of the rainy season in October 2012 will probably continue through 2013. Islamist extremists remain active in Sudan potentially threatening the security of the Sudanese Government as well as US and other Western interests.

South Sudan in 2013 will face issues that threaten to destabilize its fragile, untested, poorly resourced government. Festering ethnic disputes are likely to undermine national cohesion, and the southern government will struggle to provide security, manage rampant corruption, and deliver basic services. Despite a series of agreements in the wake of Juba's incursion into Sudan in April 2012, controversial unresolved disputes, such as the future of Abyei, risk a return to conflict between the two countries. Animosity and lack of trust between Khartoum and Juba also threaten to undermine the implementation of agreements signed in September 2012. South Sudan's economy suffered significant setbacks after Juba shut down oil production in early 2012, and it will struggle to rebound because unresolved security conflicts with Sudan have delayed the restart of oil production, despite a signed deal with Khartoum in September 2012. Ethnic conflict in South Sudan is likely to continue as the South Sudanese military struggles to disarm ethnic militias and provide security across the country. We assess the ruling Sudan People's Liberation Movement (SPLM) will continue to turn to the international community, specifically the United States, for assistance.

Somalia

Somalia's political transition in 2012 installed new political players and degraded the influence of old guard politicians responsible for corruption and mismanagement of government resources under the transitional government system. The country's nascent institutions, ill-equipped to provide social services, along with pervasive technical, political, and administrative challenges at the national level, will test Mogadishu's ability to govern effectively in 2013. Command and control of AMISOM forces and their proxies, along with facilitating cooperation between Mogadishu and AMISOM forces operating in southern Somalia, will also be distinct challenges for the government.

Al-Shabaab, the al-Qa'ida-affiliated insurgency that has terrorized populations and destabilized the transitional government since 2008, is largely in retreat, ameliorating instability and opening space for legitimate governing entities to exert control in southern Somalia. Despite its fractious state, al-Shabaab continues to plan attacks in Somalia and has returned to launching asymmetric attacks in a meager attempt to reassert control in key areas, including Mogadishu and the port city of Kismaayo. The group also poses a threat to US and Western interests in Somalia and regionally, particularly in Kenya, and leverages its operatives and networks in these locales for attacks.

Mali

In January 2012, after the return of heavily armed Tuareg fighters from Libya, the secular-based National Movement for the Liberation of the Azawad (MNLA) and the extremist Islamist Tuareg rebel group Ansar al-Din launched a rebellion against the Malian Government. Following a 21 March military coup, Ansar al-Din—with help from AQIM—and the MNLA quickly drove the Malian military out of the north. After taking control of northern Mali, AQIM worked closely with Ansar al-Din and AQIM-offshoot Movement for Tawhid and Jihad in West Africa (TWJWA) to consolidate gains in the region and impose a hard-line version of sharia.

Armed conflict between Malian Armed Forces and Islamist forces renewed in early 2013 when Islamist forces attacked Malian military outposts near Islamist-held territory. French forces quickly intervened with ground forces and airstrikes, halting AQIM and its allies' advances and eventually pushing them out of key northern Malian population centers. Regional forces and Chadian troops have begun to deploy to Mali, where European Union trainers will begin the training cycle of designated forces. Several countries have now offered significant contributions to the deploying force but lack adequate troops, training, and logistics to provide a capable force.

Mali's fragile interim government faces an uphill effort to reunite the country and hold democratic elections by mid-2013—especially elections the north perceives as credible. In addition to planning elections, local and regional actors are pursuing diplomatic options, including negotiations, to address instability in northern Mali and counter AQIM's influence.

Nigeria

The Nigerian state is acutely challenged by uneven governance, endemic corruption, inadequate infrastructure, weak health and education systems, and recurring outbreaks of sectarian, ethnic, and communal violence. Abuja also faces Boko Haram—a northern Sunni extremist group with ties to AQIM—whose attacks on Christians and fellow Muslims in Nigeria have heightened religious and ethnic tensions and raised concerns of possible attacks against US interests in the country. Communal violence is down from last year, but Boko Haram has made moves to incite it, and the Nigerian Government is scarcely addressing the underlying causes, such as socioeconomic conditions in troubled northern Nigeria, despite pledges to do so. In the Niger Delta, Abuja is struggling to extricate itself from open-ended financial commitments and has not made progress rehabilitating, retraining, and reintegrating disgruntled former militants. Militant/criminal attacks on land-based oil infrastructure in Nigeria's coastal areas, along with hijackings, kidnappings, and piracy attacks off the coast, continue at a steady pace.

Central Africa

The **Great Lakes** region of Central Africa has a total population of 128 million and includes parts or all of Burundi, Congo (Kinshasa), and Uganda. Despite gains in peace and security in the past decade, the region endures the chronic pressures of weak governance, ethnic cleavages, and active rebel groups. US Government-sponsored modeling suggests that Burundi, Congo (Kinshasa), and Uganda are all at risk of violent instability during the next year. Rwandan-backed M23 rebels in Eastern Congo in 2012 engaged the Armed Forces of Congo and UN peacekeepers in the worst fighting since 2008, displacing more than a quarter-million civilians. Other armed groups will likely increase predatory activity, encouraged by Congolese President Kabila's flawed election in 2011 and his deteriorating control. Several of these nations have become US Government security partners in recent years. Ugandan and Burundian troops compose the vanguard of AMISOM, and Rwanda is a vital part of the peacekeeping mission in Darfur.

Since 2008, Uganda has deployed troops across Congo, South Sudan, and Central African Republic to pursue Joseph Kony and the Lord's Resistance Army (LRA), with US assistance, including approximately 100 US military advisors. While LRA foot soldiers terrorize civilians in the region, Joseph Kony and his top lieutenants evade detection and tracking by keeping low profiles and moving in scattered bands across a remote region.

EAST ASIA

China

Regional Dynamics

During 2012, Beijing adopted strong, uncompromising positions in maritime territorial disputes with several of its neighbors. In each case, China sought to expand its control over the relevant territories and obstructed regional efforts to manage the disputes. Beijing's regional activities appear to be, in part, a response to the US strategic rebalance toward Asia-Pacific, which Chinese leaders believe is aimed at undermining China's position in the region. Globally, Beijing has both assisted and hindered US policy objectives on such issues as Iran, Syria, Afghanistan, and North Korea, and it continues to expand its economic influence and to try to parlay it into greater political influence.

The leadership transition in Beijing continues to unfold as Chinese leaders grapple with a confluence of domestic problems—including lagging economic indicators, corruption, and pressure for political reform—that are fueling leadership fears about the potential for serious domestic unrest.

The leadership team that is confronting these internal challenges is also likely to maintain uncompromising positions on foreign policy issues, especially those involving maritime and territorial disputes in the South and East China Seas. Meanwhile, China-Taiwan relations remained relatively calm in 2012, due in part to the continuity provided by Taiwan President Ma Ying-jeou's reelection last January. However, progress in cross-strait dialogue almost certainly will continue to be gradual, and the cross-strait military and economic balance will keep shifting in China's favor.

Military Developments

China is pursuing a long-term comprehensive military modernization designed to enable China's armed forces to achieve success on a 21st century battlefield. China's military investments favor capabilities designed to strengthen its nuclear deterrent and strategic strike, counter foreign military intervention in a regional crisis, and provide limited, albeit growing, capacity for power projection. During 2012, China's People's Liberation Army (PLA) introduced advanced weapons into its inventory and reached milestones in the development of key systems, thereby sustaining the modernization program that has been under way since the late 1990s. For example, in August, the PLA Navy commissioned the *Liaoning*, China's first aircraft carrier, which Beijing probably sees as a significant step in developing a military commensurate with great-power status. Additionally, China has continued to develop advanced ballistic missiles.

Developments in Chinese military capabilities support an expansion of PLA operations to secure Chinese interests beyond territorial issues. To expand operations—specifically in the Indian Ocean—China is pursuing more effective logistical support arrangements with countries in the region. Beijing is also maintaining a multi-ship antipiracy task force in the Gulf of Aden for the fourth straight year to protect commercial shipping. The task force operates independently of international efforts, but is making a tangible contribution to protecting shipping through this heavily pirated area.

China is also supplementing its more advanced military capabilities by bolstering maritime law enforcement (MLE) activities in support of its territorial claims in the South and East China Seas. In the territorial disputes with the Philippines and Japan last year, the Chinese Navy stayed over the horizon as MLE vessels provided Beijing's on-scene presence and response.

North Korea

Kim Jong Un has quickly consolidated power since taking over as leader of North Korea when his father, Kim Jong Il, died in December 2011. Kim has publicly focused on improving the country's troubled economy and the livelihood of the North Korean people, but we have yet to see any signs of serious economic reform.

North Korea maintains a large, conventional military force held in check by the more powerful South Korean-US military alliance. Nevertheless, the North Korean military is well postured to conduct limited attacks with little or no warning, such as the 2010 sinking of a South Korean warship and the artillery bombardment of a South Korean island along the Northern Limit Line. (For information on North Korea's nuclear weapons program and intentions, see the Proliferation section.)

RUSSIA and EURASIA

Russia

Domestic Political Developments

During the next year, Russia's political system of managed democracy will come under greater strain as the Kremlin grapples with growing social discontent and a society that is increasingly in flux. Important sectors of the Russian public are frustrated with the country's sluggish economy and are no longer content with a political system that lacks any real pluralism and suffers from poor and arbitrary governance and endemic corruption. All of these factors present Russian President Vladimir Putin with far greater challenges than any he faced during his two previous terms in office.

Putin's return to the presidency in 2012 was intended to restore strength and vigor to a system that he believed had weakened under President Dmitriy Medvedev. Instead, antipathy over the Putin-Medvedev job swap touched off some of the largest political protests Russia has seen since the breakup of the Soviet Union. Despite these unprecedented protests, the Russian leadership has demonstrated firm resolve to preserve the system, while a disparate opposition movement struggles to become more cohesive, broaden its base, and build momentum. After initially tolerating demonstrations and offering a few political reforms in the hope of dividing the opposition, the Kremlin took a more aggressive approach, adopting measures to restrict opposition activities, such as targeting opposition figures for harassment and using legislative and judicial means to confront, intimidate, and arrest opponents. These actions have helped to thwart the opposition's ability to build momentum and preserve the Kremlin's control of the political system, but they have not addressed the sources of bitterness and dissatisfaction.

Foreign Policy

Russian foreign policy is unlikely to deviate significantly from its current course in the next year, but domestic political factors almost certainly will exert greater influence on foreign policy. Putin is sensitive to any US criticisms of Russian domestic political practices, which he perceives as meddling in Russia's internal affairs. Nevertheless, he sees benefits in cooperating with the United States on certain issues.

Missile defense will remain a sensitive issue for Russia. Russian leaders are wary that in the long run US pursuit of a "missile shield" will result in systems that enable the United States to undercut Russia's nuclear deterrent and retaliatory capabilities. Russian leaders also see aspects of US plans for missile defense in Europe as serious threats to their core national security interests. The Kremlin will continue to look to the United States and our NATO partners for guarantees that any system will not be directed at Russia. On Syria, Russia is likely to remain a difficult interlocutor. The Kremlin will remain focused on preventing outside military intervention aimed at ousting the Asad regime. Moscow is troubled by the Libyan precedent and believes the West is pursuing a reckless policy of regime change that will destabilize the region and could be used against Russia. The Russians point to the rise of the Muslim Brotherhood in Egypt and the terrorist attacks against US diplomats in Libya last September as evidence supporting their arguments.

Moscow is not likely to change its diplomatic approach to Iran's nuclear program. Russia argues that confidence-building measures and an incremental system of rewards are the best ways to persuade Iran to cooperate with the International Atomic Energy Agency. Despite disagreements over missile defense and the problems of Iran's nuclear program and Syria, Moscow supports US-led NATO military operations in Afghanistan. It sees its support of the Northern Distribution Network (NDN) as a pillar of US-Russia relations that also helps stabilize Afghanistan. Nevertheless, Russia is suspicious of US intentions in Afghanistan and wary of any US efforts to maintain a residual military presence after 2014 without a UN mandate, which could put Moscow's cooperation beyond this period in doubt.

Although the bilateral relationship with the United States will remain important for Russia, Moscow is most likely to focus its foreign policy efforts on strengthening its influence over the states of the former USSR by binding them closer through integration initiatives, such as the Russia-Belarus-Kazakhstan Customs Union or Putin's proposed Eurasian Union.

The Military

Russian military forces, both nuclear and conventional, support deterrence and enhance Moscow's geopolitical clout. Since late 2008 the Kremlin has embraced a wide-ranging military reform and modernization program to field a smaller, more mobile, better-trained, and high-tech force during the next decade. This plan represents a radical break with historical Soviet approaches to manpower, force structure, and training. The initial phases, mainly focused on force reorganization and cuts in the mobilization base and officer corps, have been largely implemented and are being institutionalized. The ground forces alone have reduced about 60 percent of armor and infantry battalions since 2008, while the Ministry of Defense cut about 135,000 officer positions, many at field grade.

Moscow is now setting its sights on long-term challenges of rearmament and professionalization. In 2010, a 10-year procurement plan was approved to replace Soviet-era hardware and bolster deterrence with a balanced set of modern conventional, asymmetric, and nuclear capabilities. However, funding, bureaucratic, and cultural hurdles—coupled with the challenge of reinvigorating a military industrial base that deteriorated for more than a decade after the Soviet collapse—complicate Russian efforts.

The reform and modernization programs will yield improvements that will allow the Russian military to more rapidly defeat its smaller neighbors and remain the dominant military force in the post-Soviet space, but they will not—and are not intended to—enable Moscow to conduct sustained offensive operations against NATO collectively. In addition, the steep decline in conventional capabilities since the collapse of the Soviet Union has compelled Moscow to invest significant capital to modernize its conventional forces. At least until Russia's high precision conventional arms achieve practical operational utility, Moscow will embrace nuclear deterrence as the focal point of its defense planning. It still views its nuclear forces as critical for ensuring Russian sovereignty and relevance on the world stage and for offsetting its military weaknesses vis-à-vis potential opponents with stronger militaries.

The Caucasus and Central Asia

Recent developments in **Georgia,** following the victory of Prime Minister Bidzina Ivanishvili's Georgian Dream party in the October 2012 parliamentary elections, offer new hope for easing bilateral Russian-Georgian tensions. Prime Minister Ivanishvili has expressed interest in normalizing relations with Russia and has sought to improve the tone of the dialogue with Moscow. However, after nearly a decade of President Mikheil Saakashvili's United National Movement party rule, Georgia faces a challenging political transition and an increased risk of domestic political instability.

The standoff between **Armenia** and **Azerbaijan** over the Armenian-occupied Nagorno-Karabakh region remains a potential flashpoint. Heightened rhetoric, distrust on both sides, and recurring violence along the Line of Contact increase the risk of miscalculations that could escalate the situation with little warning.

The threat of instability remains in the states of **Central Asia**. Central Asian leaders have prioritized regime stability over political and economic reforms that could improve long-term governance and legitimacy. Most fear any signs of Arab Spring-type uprisings and repress even small signs of discontent. The Central Asian states have not built constructive relationships with each other; personal rivalries and longstanding disputes over borders, water, and energy create bilateral frictions between neighbors and potential flashpoints for conflict. Ethnic conflicts are also possible and could emerge with little warning. Clashes between ethnic Uzbeks and Kyrgyz in southern Kyrgyzstan following the 2010 overthrow of the government resulted in the deaths of more than 400 people, and in the absence of government efforts to lead reconciliation, tensions between these ethnic groups remain high.

Ukraine, Belarus, and Moldova

In **Belarus,** Lukashenko has weathered an economic crisis that presented him with the greatest challenge to his rule since he took power in 1994. Corrective measures and financial assistance from Russia have eased some of the more harmful consequences of the crisis, and opposition movements, such as the Revolution through Social Networks, have petered out. Nevertheless, Belarus's economic situation remains precarious, and Lukashenko's refusal to institute structural economic reforms raises the likelihood that Belarus will fall into another economic crisis in 2013.

Under President Yanukovych, **Ukraine** is drifting towards authoritarianism. The October 2012 parliamentary elections were marred by irregularities and fell far short of Western standards for free and fair elections, representing a step backwards from prior Ukrainian elections. Yanukovych also shows few signs that he intends to release imprisoned opposition leader former Prime Minister Yuliya Tymoshenko any time soon, a key condition to improving Ukraine's relations with the West. The government appears to be "doubling down," preparing additional criminal charges against Tymoshenko that could keep her behind bars for life. In addition, the lack of structural economic reforms coupled with a precarious financial situation raises the risk of economic crisis in 2013.

The status quo in **Moldova** is likely to prevail during the next year. Electing new leaders in Moldova and in the separatist region of Transnistria has improved the tone of relations between Chisinau and Tiraspol. A renewed focus on confidence-building measures, such as easing restrictions on the movement of people and goods, generated cautious optimism in early 2012 about progress toward eventual settlement of the Transnistria conflict. However, the negotiating positions of both sides later hardened, and a settlement to the conflict is highly unlikely in the next year.

LATIN AMERICA and THE CARIBBEAN

Positive trends in much of Latin America include the deepening of democratic principles, economic growth, and resilience in the face of the global financial crisis. Income inequality in the region is also showing a steady decline. In some areas, however, economic stagnation, high rates of violent crime and impunity, ruling party efforts to manipulate democratic institutions to consolidate power, and slow recovery from natural disasters are challenging these strides. Initiatives to strengthen regional integration are leading some countries to try to limit US influence, but they are hampered by ideological differences and regional rivalries.

Iran has been reaching out to Latin America and the Caribbean to decrease its international isolation. President Ahmadinejad traveled to the region twice in 2012. Tehran has cultivated ties to leaders of the Venezuelan-led Alliance for the Peoples of our Americas (ALBA) in Bolivia, Cuba, Ecuador, Nicaragua, and Venezuela, and maintains cordial relations with Cuba and Nicaragua. Relations with Tehran offer these governments a way to stake out independent positions on the international issue of Iran, while extracting financial aid and investment for economic and social projects.

The drug threat to the United States emanates primarily from the Western Hemisphere; the overwhelming majority of drugs now consumed in the United States are produced in Mexico, Colombia, Canada, and the United States. Patterns in drug marketing and trafficking create conditions that could fuel this trend and further undermine citizen security in several countries in the region. Central American governments, especially Honduras, El Salvador and Guatemala, are trying to cope with some of the highest violent crime and homicide rates in the world. In addition, weak and corrupt institutions in these countries foster permissive environments for gang and criminal activity, limit democratic freedom, encourage systemic corruption, and slow recovery.

Mexico

Recently inaugurated Mexican President Enrique Peña Nieto inherited a complex security situation marked by confrontation between the state and drug cartels, strong public concern over levels of violence, and unprecedented security cooperation with the United States. Peña Nieto has said he will prioritize efforts to reduce violence and push reforms aimed at strengthening the rule of law, including: Mexico's transition to an accusatory system of justice, a more effective counter-illicit finance regime, police professionalization, and bolstered government intelligence capabilities.

President Calderon turned over the presidency to Peña Nieto on 1 December, having made headway against several cartels, in particular Los Zetas, the Beltran Leyva Organization, and the Gulf Cartel. Drug-related homicides have increased significantly since 2007—Calderon's first full year in office—and remain high; more than 50,000 Mexicans have died as a result of drug-related violence since that year.

Peña Nieto promised to push forward Calderon's landmark 2008 constitutional reform to overhaul Mexico's judicial system. The judicial reform process has been uneven across Mexico's states, and many are unlikely to meet the 2016 implementation deadline. On police reform, Peña Nieto plans to create a new gendarmerie, or paramilitary police, to gradually take over policing duties from the military. He also has publicly endorsed efforts to reform and modernize the federal police, as well as state and municipal-level police forces. Peña Nieto's plans to emphasize anti-money laundering efforts will be strengthened by a recently passed law that restricts high-value dollar and peso purchases commonly used to launder drug proceeds, such as in real estate sales, and requires government entities to provide data to support money-laundering prosecutions.

Venezuela

Venezuelan President Hugo Chavez's death on 5 March has triggered preparations for a new election in which we expect Vice President Nicolas Maduro to compete against Miranda Governor and former presidential candidate Henrique Capriles Radonski. Venezuelan Foreign Minister Elias Jaua announced that Maduro will take over as interim president and that an election will be held within 30 days. Maduro is a long-time Chavez loyalist and will almost certainly continue Chavez's socialist policies.

The Venezuelan Government will be up against the consequences of an increasingly deteriorating business environment and growing macroeconomic imbalances. Debt obligations will consume a growing share of Venezuela's oil revenues, even if oil prices remain high. Lingering citizen concerns that Caracas will face in the next year also include personal safety, which has been threatened by a rising tide of violent crime.

Cuba

Cuban President Raul Castro is proceeding cautiously with economic reforms to reduce the state's direct role in the economy and diversify trade relations, while preserving socialism and the regime. Measures implemented since 2011 to expand self-employment, permit sales of vehicles and property, and lease state lands to farmers are generally popular but have failed to produce much growth. With their primary patron Hugo Chavez's death, Cuba's leaders are urgently trying to attract foreign investment partners and increase their access to hard currency and foreign credit.

A priority for Cuban leaders is ensuring that economic reform does not increase pressure for a political opening and greater individual rights. There is no indication that Castro's efforts, including his stated interest in laying the groundwork for a generational transition in leadership, will loosen the regime's grip on power. The stiff prison term imposed on USAID subcontractor Alan Gross for facilitating uncensored Internet connectivity demonstrates the Castro regime's sensitivity to public access to technology and information beyond its control. Indeed, harsh government repression of peaceful protests and an upswing in short-term arrests of dissidents indicate economic changes will not be coupled with political changes.

Havana recently announced a new travel and migration policy for most Cubans that will no longer require exit permits and extends the time Cubans can remain abroad without forfeiting property and other rights. The new policy has thus far only prompted a modest boost in US visas. The US Interests Section in Havana recently implemented process improvements that dramatically reduced wait times for non-immigrant visa appointments. Countries around the region are watching for any indication of significant increases in Cuban nationals arriving under the new travel policy, but to date they have seen no such increases.

Haiti

Stability in Haiti is fragile because of the country's weak governing institutions. Strained relations between President Michel Martelly, in office since May 2011, and the opposition-dominated legislature are delaying progress on several fronts, including plans to hold overdue Senate and local elections and advance the President's agenda to create jobs, improve education, and attract foreign investment. Although Martelly is generally still popular, the risk of social unrest could grow because of unmet expectations over living conditions and the lack of economic opportunities. President Martelly will likely face continued protests—some possibly violent and organized by his enemies—over rising food costs.

President Martelly and Prime Minister Laurent Lamothe intend to prioritize private-sector-led growth and end dependence on aid. However, Haiti will remain dependent on the international community for the foreseeable future because of the devastating effects of the earthquake in January 2010 on infrastructure and production capacity, several recent natural disasters that ruined staple food crops, and the unsettled political and security climate. Of the estimated 1.5 million Haitians displaced by the earthquake, more than 350,000 are still in tent encampments. We assess that the current threat of a mass migration from Haiti is relatively low because Haitians are aware of the standing US policy of rapid repatriation of migrants intercepted at sea.

EUROPE

Euro-Zone Crisis

European leaders are still grappling with the euro-zone crisis—the euro zone's economy slipped back into recession in 2012 following two years of slow economic growth. We noted last year that the outcome of the crisis has major implications not just for the United States but also for the world economy. The risk of an unmanaged breakup of the euro zone is lower this year because European Union (EU) leaders have taken steps to strengthen banking and fiscal integration, but economic deterioration in Europe threatens to depress world growth.

This year, rising anger over austerity could affect Europe's social and political fabric. Given high unemployment—particularly among youth—throughout the peripheral euro-zone states (Greece, Italy, Portugal, and Spain), there has been an uptick in strikes and violent protests. The greatest risk to stability is austerity- and reform-fatigue spreading across Europe. In November 2012, tens of thousands marched—mostly in southern Europe but also in Belgium and France—in the first pan-EU labor union action against budget cuts. The crisis has already led most European states to cut defense spending, reducing the capability of Allies to support NATO and other US security interests around the world.

Turkey

Turkey's activist foreign policy has changed fundamentally during the past year, mostly in reaction to Asad's brutal approach to the opposition-led unrest in Syria. Ankara has since begun to support overtly the Syrian political opposition by hosting its members in Turkey. This is a departure from Turkey's ruling Justice and Development party (AKP)-designed foreign policy approach, which emphasized engagement and incentives for shaping behavior but is now driven by the destabilizing regional effects of the Asad regime's actions. Turkey continues to call on the international community to take action against Asad and is increasingly turning to the United States and NATO for assistance in managing the crisis.

The Turkish Kurdish terrorist group Kurdistan People's Congress (KGK/former PKK) is Ankara's primary security threat. Turkey's Kurdish issue, marked by armed struggle against insurgent KGK forces now entering its fourth decade, is increasingly challenging Ankara domestically with regional implications. KGK-initiated violence inside of Turkey is at its deadliest level in more than a decade. This development is fueling public opposition to much-needed constitutional reforms to address the Turkish Kurdish minority's legitimate demands for political and cultural rights. The sharp rise in violence has pushed Ankara to lean more toward military, vice political, means to deal with the KGK, although efforts are under way to re-launch talks with the KGK leadership. Kurds in Syria are taking advantage of unrest fomented by the opposition to Asad, which is stoking Turkish fears of Kurdish separatism in Turkey.

Turkish relations with Iraq are strained. Turkish leaders are concerned about what they perceive to be increasingly authoritarian tendencies of the Maliki-led government, relations among communities within Iraq, and perceived trends in Iraq's foreign policy. Iraq has been angered by Turkey's efforts to expand political and energy ties with Iraq's semi-autonomous Kurdistan Region without consulting Baghdad.

The Turkey-Israel bilateral relationship remains troubled. In a September 2012 speech, Erdogan said Turkey would not normalize relations with Israel until Israel met Ankara's three conditions: publicly apologizing for the 2010 incident in which Israel interdicted an aid flotilla headed for Gaza and killed nine aboard the ship Mavi Marmara; providing reparations to the families of the Mavi Marmara victims; and lifting the Gaza blockade. Israel's late 2012 operation against HAMAS and other Palestinian militant groups in Gaza further hardened Turkish attitudes. There seem to be few prospects for improving relations between Israel and Turkey.

The Balkans

Ethnic and internal political divides in the **Western Balkans** will continue to pose the greatest risk to regional stability in 2013. Many fragile states in the region suffer from economic stagnation, high unemployment, corruption, and weak rule of law. Although the security situation in Kosovo's Serb-majority north has improved since fall 2011, Western diplomatic and security engagement is needed to implement many of the agreements reached in EU-sponsored talks.

As the EU-facilitated dialogue to help normalize relations between **Kosovo** and **Serbia** gains traction, the risk of threats and violence by ethnic Serb hardliners in northern Kosovo probably will increase. Serbia gained EU candidacy status in March 2012 and would like a date to begin EU accession talks. However, the relatively new government (elected last May) faces large hurdles in fulfilling EU accession criteria and reconciling Serbia's constitutional claims to Kosovo with the fact that Kosovo is independent. Kosovo's supervised independence ended in September 2012, and Pristina will likely seek to expand its instruments of sovereignty over its territory. The Kosovo Government opened the Mitrovica North Administrative Office in July 2012, extending government services to the Serb-majority region. In June 2013, Kosovo law allows the government to change the mandate of Pristina's potential efforts to transition the Kosovo Security Force (KSF). This warrants attention to avoid negative responses from Belgrade and the Kosovo Serb community in northern Kosovo.

In **Bosnia-Herzegovina** (BiH), differences among Serb, Croat, and Bosniak elites are intensifying, threatening BiH's state institutions and posing obstacles to further Euro-Atlantic integration. A series of political crises have distracted attention from pursuing needed reforms for EU and NATO integration, and secessionist rhetoric from the leadership of the political entity Republika Srpska has further challenged Bosnia's internal cohesion. In **Macedonia**, we do not expect a return to the civil war violence of a decade ago. However, disputes between Albanian and Macedonian communities might become more polarized in the coming year. Tension between Macedonia and **Bulgaria** warrants attention. In addition, Greece's ongoing objection to the country using the name "Macedonia" is another source of friction, and blocks Macedonia's EU and NATO aspirations. In **Albania**, government institutions suffer from corruption and excessive political influence. In the lead-up to the June 2013 parliamentary elections, there is worry about a return to the heated, partisan conflict that erupted after the 2009 parliamentary elections, when the opposition party contested the election and boycotted parliament on-and-off for nearly two years.